دولة ليبيا

وزارة التعليم العالى والبحث العلمى

جامعة سبها

كلية تقنية المعلومات

قسم الشبكات

بحث مقدم لاستكمال متطلبات نيل درجة البكالوريوس

تحت عنوان:

مراقبة وتحليل شبكة جامعة سبها بواسطة محلل الشبكة (Wireshark)

Monitring And Analyzing The Sebha University Network by The Network Analyst (Wireshark)

إعـــــــداد الطالبان:

حـمـد ابوعقيلـة مسعـود

20170139

عبدالرحمن الفيتوري عبدالرحمن

20170106

تحـت إشراف: د.مـاهر عبدالله الغالــي

للعام الجامعي

2023-2022

إقرار

إقرار الطالب / الطلاب

أنا الطالب : حمد أبوعقيلة مسعود **الرقم الدراسي:20170139**

أنا الطالب : عبدالرحمن الفيتوري عبدالرحمن **الرقم الدراسي:20170106**

نقر بإن ما ورد في هذا البحث هو من مجهودنا الشخصي ماعدا الفقرات التي تم إسنادها إلى مرجع.

التاريخ:..... التوقيع:.....

إقرار المشرف

اسم المشرف :د. ماهر عبدالله الغالي.

أقر بأني اطلعت على مادة البحث، وأن البحث جاهز للمناقشة.

التاريخ: ..... التوقيع:.....

إقرار بالموافقة على التصحيحات وتسليم النسخة النهائية:

بعد التصحيح والاطلاع على مادة البحث، تمت الموافقة عليها، وتسليم النسخة النهائية.

اسم الممتحن الأول:.....التوقيع:.....التاريخ: .....

اسم الممتحن الثاني:.....التوقيع:.....التاريخ: .....

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

﴿ قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا ۖ إِنَّكَ أَنتَ الْعَلِيمُ الْحَكِيمُ ﴾

{ البقرة: 32 }

الأهداء

الي بلسم الحياة وينبوع العطاء الذي زرع في نفسي الطموح والمثابرة وحصد الشوك عن دربي، الي من علمني ان الدنيا كفاح وسلاحها العلم والمعرفة الي الذي لم يبخل علي باي شيء، الي من سعى لاجل راحتي ونجاحي، الي من اهلكته الحياة واحنت ظهره الايام لوصولي الي ما انا عليه الان.

((الي اعظم واعز رجل في الكون))

ابـــي العزيــز

الي الحنان الرباني والنبع الاحساني الي التي سهرت وتعبت لأرتاح وشقيت لأسعد الي التي يرحمنا الله لاجلها الي من ساندتني في صلاتها ودعائها ومالها وعافيتها الي التي انارت دربي بنصائحها الي من علمتني الصبر والاجتهاد ومنحتني القوة والعزيمة لمواصلة الدرب الي نبع العطف والحنان الي اجمل ابتسامة في حياتي.

((الي اروع والطف انثى علي وجه الارض))

امـــي الغاليـة

الي الشموع الموقده التي تنير ظلمة حياتي الي من بوجودهم اكتسبت قوة ومحبة لاحدود لها اخواني واخواتي.

الي من ساندوني في الصغيرة والكبيرة الي من وقفو معي في كل محنة أمر بها الي من كانو لي اهل واخوة شكرا لتلك السنين الي قضيتها برفقتكم كنتم خير اصدقاء.

((شكراً لكم جميعا))

كلمـــة شـــكر

إلـــــهي

انت البداية .....وانت النهاية.....وانت كل شي.

لك الشكر علي نعمة البصر اولاً، ثم نعمة العقل ،ثم نعمة الصحةالتي اكتملت بها كل النعم الأخرى، منها نعمة العلم.

الي معلمي الذي لم اراه، الي سيد الخلق إمام المرسلين، والي سيد الخلق إمام المرسلين،الي الأمي الذي علم المؤمنين إليك يا سيد الأنبياء والمرسلين سيدنا

محمد صلى الله عليه وسلم

بعد ذلك أتقدم بجزيل الشكر وعظيم الامتنان إلى كل من:

الدكتور الفاضل: ماهر الغالي على تفضله الكريم بالاشراف علي هذه الدراسة وعلى كل ماقدمه من توجيهات ومعلومات ساهمت في أثراء الدراسة في جوانب مختلفة.

رئيس القسم: أ.محمود حفص الدين علي كل ماقدمه من مجهودات وتوجيهات.

أستاذة الفاضلة: أ.سلوى عبدالنبي على ماقدمته من فضل وعطاء ومساندة لتوصلنا إلى هذا المستوى العلمي.

كما اتقدم بخالص الشكر والامتنان الي لجنة المناقشة علي قبولهم لمناقشة هذه الدراسة البحثية، وايضاً موظفين مركز تقنية معلومات جامعة سبها، وأعضاء هيئة التدريس الذين ساهموا في إنجاز هذه الدراسة.

فهرس المحتويات

فهرس الأشكال

(فهرس الجداول)

فهرس المصطلحات

المصطلح باللغة العربية	المصطلح باللغة الإنجليزية	الإختصار
قراصنة القبعة السوداء	Black Ha	–
قراصنة القبعة الرمادية	Greay Ha	–
شبكة	Network	–
حركة المرور	Traffic	–
التقاط أو استنشاق	Sniffing	–
حزمة	Packet	–
مفتوح المصدر	Open Source	–
هجوم خداع ARP	ARP poisoning	–
هجوم حجب الخدمة	DOS Attack	–
هجوم الفيضان MAC	MAC Flooding	–
انتحال اسماء النطاقات	DNS Spoofing	–
التقاط حزمة	Sniffer Packet	–
طبقة الربط	Link Layer	–
نواة	Kernel	–
سلك	Wire	–
مجموعة	Collection	–
التحويلات	Conversion	–
تحليل	Analysis	–

الفصل الاول

مقدمة البحث

المقدمة:

يشير مفهوم شبكات الحاسوب إلى الأسلوب المستخدم في توصيل وربط مجموعة من الأجهزة والموارد مع بعضها البعض، حتى تتيح لمستخدمي هذه الموارد الأتصال ومشاركة المعلومات والملفات مع بعضهم البعض من أي مكان وفي أي وقت حسب طبيعة الشبكة وحجمها، وحسب نوع الخدمة التي يجب أن توفرها المؤسسة أو الشركة التي ستعمل عليها الشبكة، وفي ظل استمرار الشبكات في النمو من حيث حجم البيانات والمعلومات وتزايد الطلب عليها من قبل المستخدمين، فأنه يجب أن تتوفر فيها عملية مهمة ومحورية جداً لضمان أستمرار عمل هذه الشبكات من دون وجود اي مشاكل أو أخطاء قد تؤدي إلى توقفها، وهذه العملية بتأكيد هي عملية المراقبة.

حيث تعاني الكثير من الشبكات من مشاكل متعددة وكبيرة في جانب المراقبة، وهذا لصعوبة أكتشاف هذه الأخطاء التي من الممكن أن تحدث بفعل فاعل أو بغير قصد، ويرجع السبب في ذلك إلى عدم التخطيط والأختيار الجيد للبرامج التي سيتم عن طريقها مراقبة وتحليل الشبكة بعد دخولها إلى العمل إثناء عملية التخطيط لبناء الشبكة، حيث يجب أن يتم في هذه المرحلة توفير طرق وبرامج مناسبة وفعالة جداً لمراقبة الشبكة وتحليلها، لضمان عملها بشكل جيد من دون وجود مشاكل أو أخطاء قد تسبب في توقفها أو أختراقها أمنياً، لهذا السبب تم تصميم برامج متخصصة في إدارة وتحليل الشبكة، من أشهرها (OpenNMS) و(Wireshark) و(Nagios) و(Observium)، حيث تساعد هذه البرامج في تقليل إمكانية حدوث أي مشاكل في الشبكة أو إنقطاعها عن العمل وتقليل التكاليف المالية المترتبة على ذلك، وكذلك توفير الكثير من الوقت والجهد.

حيث تواجه شبكة جامعة سبها مشكلة في عدم وجود أي برنامج أو نهج مراقبة وتحليل واضح بشكل دوري، ليتم بعدها معرفة حالة الشبكة، أن كانت معرضة لتعطل أو التوقف أو بها مشكلة ما، ومعرفة الأسباب التي أدت لظهور هذه المشكلة بشكل سريع لإختصار الوقت، ومعالجة هذه المشكلة في أسرع وقت ممكن، لتسهيل العملية الدراسية بالنسبة لطلبة الجامعة وعملية العمل والإدارة بالنسبة لأعضاء هيئة التدريس وموظفي الجامعة، لذا يجب أن يكون هناك أسلوب متبع لمراقبة وتحليل الشبكة للوصول لأي مشكلة تحدث للشبكة، ومن هنا جائت فكرة الدراسة الحالية التي تهدف لأستخدام برنامج (Wireshark) لمراقبة شبكة جامعة سبها، حيث يعتبر هذا البرنامج من أفضل البرامج الفعالة والمستخدمة عالمياً لتحليل حركة المرور بشكل كلي داخل الشبكة، فهو مجاني ومفتوح المصدر، كما أنه متوافق مع جميع أنظمة التشغيل الأساسية، ويتم أستخدامها

على نطاق واسع في الشبكة، لحل مشكلة الأداء الخاص بالشبكة، وكما يمكن أستخدامها بطريقة تعليمية في شرح طريقة عمل الشبكات من قبل الفنين واعضاء هيئة التدريس [1].

حيث تركز هذه الدراسة على مراقبة وتحليل شبكة جامعة سبها بشكل عام وشبكة كلية تقنية المعلومات وكلية العلوم بشكل خاص بإستخدام (Wireshark)، حيث تم اختيار وتحديد وتقسيم المكان الذي سيجرى فيه البحث بين موظفي وأجهزة مبني مركز تقنية المعلومات، وأجهزة موظفي كلية تقنية المعلومات، والوقت الذي تم فيه جمع البيانات في اوقات عمل الموظفين قبل بداية الدراسة وبعدها، ومعرفت أيضاً ما إذا كانت الشبكة تتعرض لحمل زائد وأسباب هذا الحمل، والوصول إلي امكانية استغلال الشبكة بصورة أفضل، ومعرفة أيضاً ما إذا كانت الأجهزة بحاجة لتطوير أو تحديث، وإمكانية معرفة ما إذا كان هناك أي عملية أختراق او تنصت خارجية للشبكة من قبل مخترقين (Black Hat) و(Greay Hat).

1.1 مشكلة البحث Research problem

ومن خلال مقابلة شخصية مع مدير مركز تقنية المعلومات جامعة سبها، أتضح أن شبكة جامعة سبها تعاني من مشاكل في عملية التحليل والمراقبة، ومن أهم المشاكل التي تعاني منها:

1. لا يوجد مراقبة أو نهج واضح ومتبع لمراقبة وتحليل الشبكة بشكل كامل وجمع وتحليل كافة البيانات وعرضها بتنسيق يسهل استخدامه.
2. عدم التأكد من ان البروتوكولات التي تتواجد في الشبكة الداخلية بأنها خالية من الثغرات التي يمكن ان يتم استغلالها بشكل غير أمن من أطراف خارجية.

2.1 أسئلة البحث Research Question

1. هل بالإمكان حل مشاكل تجميع وتحليل البيانات الخاصة بالشبكة وعرضها بتنسيق مبسط ومفهوم لاستخدامها في عملية الحل؟
2. هل يمكن التأكد من أن البروتوكولات التي تتواجد في الشبكة الداخلية بأنها أمنة وخالية من الثغرات؟

3.1 أهداف البحث Research Objective

تهدف هذه الدراسة إلى:

1. معرفة الأعطال والمشاكل التي تحدث في الشبكة وتحديد موقعها عن طريق استخدام برنامج محلل الحزم (Wireshark).
2. التأكد من أن البروتوكولات التي تتواجد في الشبكة الداخلية بأنها أمنة وخالية من الثغرات.

4.1 اهمية البحث Importance of research

ترجع أهمية هذه الدراسة الي تجميع وتحليل ومراقبة البيانات الخاصة بشبكة جامعة سبها، بواسطة محلل الشبكة (Wireshark)، وذلك لغرض توفير حلول للمشاكل التي تعاني منها الشبكة الحالية، من حيث عدم وجود اي برامج او نهج متبع لعملية المراقبة.

5.1 الدوافع

هناك دافعين لتبني هذا البحث، الدافع الاول للمصلحة العامة وثاني للمصلحة الشخصية، الدافع العام هو تحسين جودة الشبكة والحصول على شبكة قوية وعملية بشكل سلسل، من اجل ان يحصل طلبة الفصول القادمة على شبكة تعليم اقوى وافضل من التي كانت لدينا في فترة الدراسة، الدافع الشخصي هو استغلال العلم الذي لم يبخل به اساتذتنا اثناء الدراسة في قسم الشبكات بشكل عملي، حتا نفهم بشكل افضل هذا العلم ونحصل منه علي خبرة كافية.

6.1 نطاق البحث Proposed Scope

مراقبة وتحليل شبكة جامعة سبها بإستخدام برنامج **(Wireshark)**، الذي يقدم الكثير من الخدمات لمراقبة الشبكة، ومعرفة انواع البيانات التي تمر بين أجهزة الشبكة، ووجهات هذه البيانات عند خروجها من الشبكة، وأيضاً إمكانية معرفة انواع البروتوكولات التي تنقل هذه البيانات، ومعرفة ايضاً أوقات الذروة الخاصة بالشبكة، وحجم الأستهلاك، ومتوسط الحجم الأجمالي، وكذلك عدد البيانات الإجمالي ومتوسطها.

7.1 النتائج المتوقعة Expected results

1. تسهيل عملية تحليل ومراقبة شبكة جامعة سبها.
2. معرفة انواع البروتوكولات المستخدمة والتأكد من انها أمنة.
3. معرفة مصدر البيانات والوجهة التي ستذهب اليها.
4. معرفة اوقات الذروة الخاصة بالشبكة.

8.1 هيكلية البحث Research Structure

- **الفصل الأول:** يتم فيه التحدث عن مفهوم الشبكة (Network) واهمية المراقبة والتحليل للشبكة من اجل ان تعمل بصورة صحيحة ولا تتعرض لعمليات التوقف المتكررة و للمحافظة عليها من عمليات التنصت و الاختراق.
- **الفصل الثاني:** ذكر فيه الدراسات السابقة المتعلقة بعملية مراقبة وتحليل الشبكة، وأهمية برنامج (Wireshark) لمراقبة الشبكات لفهم حالة الشبكة.
- **الفصل الثالث:** يتناول فيه تعريف ببرنامج (Wireshark) والأدوات المستخدمة في عملية المراقبة.
- **الفصل الرابع:** يتناول تعريف بالمنهجية المستخدمة.
- **الفصل الخامس:** يتناول الجانب العملي.
- **الفصل السادس:** يتظمن مناقشة النتائج التي تم التوصل اليها بتطبيق هذا المشروع و الخلاصة والصعوبات والعراقيل والأبحاث المستقبلية.

الفصل الثانـي

الدراسات السابقة

2.الدراسات السابقة:

من المعروف بشكل عام أن مفهوم شبكات الحاسوب بسيطة إلى حد ما، الا انها صعبة عند التنفيذ، حيث أنه عند الإنتهاء من تصميم وتنفيذ الشبكة وإدخالها للعمل من الطبيعي ان تحدث فيها عدة اخطاء بقصد أو دون قصد، نتيجة لعدم التخطيط الجيد لبعض الأجزاء في الشبكة التي وقعت فيها هذه الاخطاء، حيث يعتبر إكتشاف مشاكل الشبكة وحلها من أهم الصعوبات التي تواجه مدير الشبكة، لذلك تعتبر عملية مراقبة الشبكة عن طريق التخطيط والاستعداد لحدوث أي مشاكل أفضل بكثير من الإنتظار الي عند حدوث المشكلة وإصلاحها، ووفقا لما ذكره [2] إن عملية المراقبة هي عملية فحص شامل لنظم والخدمات التي تتكون منها الشبكة، لذلك من المهم البحث عن أساليب منظمة وواضحة تساعد على رصد وقياس وابلاغ ومتابعة وتقديم تقارير عن صحة وجودة البنية التحتية الخاصة بالشبكة، حيث يسمح هذا الأجراء لمدير الشبكة بالحفاظ على الشبكة بحالة جيدة وقابلة بسهولة للتحسين والتطوير مستقبلا، حيث أنه بعد الإنتهاء من تكوين وتهيئة الأجهزة ومعدات الخاصة بالشبكة، يأتي بعدها أمر مهم جداً وهو في غاية الأهمية، ألا وهو مراقبة كافة الموارد المشغلة لشبكة، والتي تعتبر أحد الأنشطة المهمة في إدارة الشبكة، حيث يجب إدارة ومراقبة الخوادم التي تعمل بشكل مستمر وصيانة المباشرة للمشاكل التي قد تحدث، سواء كانت هذه الخوادم خوادم فعلية، أو خوادم إفتراضية، حيث إن أغلب الشبكات لديها مشاكل في مراقبة الخوادم قيد التشغيل، وذالك بسبب عدم وجود نهج واضح ومتبع لعمل برامج المراقبة، حيث أن أغلب البرامج المستخدمة تعمل بشكل عشوائي لا يتناسب مع البيئة والشبكة التي يعمل عليها حسب ما ذكره [3]، لذلك يجب توفير برامج وأدوات تعمل بنهج واضح يتناسب مع الشبكة التي سيراقبها بإقل تكاليف مالية ممكنة واطول وقت.

ومع التطور والتقنيات الحديثة تزداد الشبكة في النمو بشكل كبير وعدد المستخدمين في شبكة يتزايد يوم بعد يوم مما ينعكس على نمو وتزايد (Traffic) حركة مرور الشبكة ايضاً، لذلك من المهم جداً مراقبة (Traffic) للحفاظ على الشبكة، وبالنسبة للشبكات العملاقة تعتبر مراقبة الشبكة مهمة معقدة للغاية، بسبب الكمية الكبير من الحزم، ولهذا السبب يتم القيام بالإستنشاق (Sniffing) للحزمة (Packet)، وتعتبر عمليات (Sniffing) أمر مُهم للشبكة لمراقبة أنشطة الشبكة التي تساعد مسؤولي الشبكة علي اكتشاف ضعف الموجود فيها، وفي دراسة[4] تم التركيز علي القيام بعملية (Sniffing)

لحركة المرور (Traffic) في بيئات مختلفة للشبكة لمساعدة مسؤولي الشبكة علي اكتشاف ضعف الشبكة بإستخدام أداة محلل الحزم (Wireshark)، هذه الأداة تمكن محلل الشبكة من تحليل (Traffic) الخاص بالشبكة للعديد من البروتوكولات مثل (TCP) و (UDP) و (IP) وغيرها الكثير.

ونظرا لتعقيدات والصعوبات التي تواجه الشبكات، عادة مايقوم مسؤولي الشبكة بدمج العديد من الأدوات مع بعضها البعض لبناء بيئة مراقبة شاملة تلبي كافة متطلبات الشبكة، وفقاً لما ذكره [5]، يمكن التفكير في برنامج محلل حزم الشبكة (Wireshark) كجهاز قياس يمكن ان يستخدم لتحليل ومراقبة كافة العمليات التي تحدث في الشبكة، حيث يقوم بإلتقاط حزم الشبكة ويحاول عرض أكبر قدر من التفاصيل عن هذه الحزم، ويعتبر (Wireshark) واحدة من أفضل أدوات تحليل الحزم المجانية ومفتوحة المصدر(Open Source) المتاحة اليوم، والذي يتم إستخدمه من قبل مسؤولي الشبكة لاستكشاف كافة مشاكل الشبكة وإصلاحها، وكذلك التحقق من وجود مشاكل أمنية لإلتفات إليها بشكل فوري، قبل أن تتفاقم المشكلة.

وفقاً لما ذكره [6] إن محلل الحزم (Wireshark) يعرف علي أنه برنامج مجاني ومفتوح المصدر، يستخدم لأستكشاف الأخطاء التي تحدث في الشبكة، وكذلك لتحليل ملفات البيانات، كما يستخدام أيضاً في التقاط حركة مرور البيانات والبروتوكولات التي تمر عبر الشبكة، ومعرفة عمليات إرسال وإستقبال البيانات بين أجهزة الشبكة.

ومن المؤكد إن إزدحام البيانات يمكن أن يكون مصدر قلق أو خطر على مسؤولي الشبكة، وفي الغالب قد يؤدي هذا الازدحام إلى الضغط بشكل كبير جداً على موارد الشبكة وقد يؤدي إلى توقفها عن العمل، حيث يمكن ان يتسبب ذلك في مشاكل عديدة، مثل فقدان الاتصال وإنخفاض الأداء وتوقف الشبكة وغيرها من المشاكل الأخرى، وغالباً لا يتم التعرف على المشاكل التي وقعت بسبب بنية الشبكة الخاطئة، ومع ذلك في بعض الأحيان قد يكون السبب في توقف الشبكة هو الهجمات الخارجية، التي تحاول تعطيل خادم الويب الخاص بالمؤسسة المقدمة للخدمة، عن طريق إرسال حزم الرد (ARP) الخاطئة أو بإصابة الشبكة باستخدام البرمجيات الخبيثة.

وتعد الخطوة الأولى في إتخاذ الإجراءت المناسبة في هذه الحالات هي تحديد مصادر الهجوم، حيث يمكن بأستخدام (Wireshark) مراقبة حركة مرور (traffic) الخاصة بالشبكة، وتوضح ايضاً كيف يمكن أن يكون (Wireshark) مفيداً للغاية، وكيف يمكن عن طريقه إكتشاف الهجمات التي تحدث للشبكات المحلية المختلفة، مثل هجوم (ARP poisoning،DOS Attack،MAC Flooding، DNS Spoofing)، وكما يمكن أيضاً بإستخدام (Wireshark) توفير بعض التقنيات التي يمكن من خلالها تخفيف هذه الهجمات، وفقاً لما ذكره [7].

وفقا لما ذكره [8] ان برنامج (Wireshark) يوفر لمهندس الشبكة مجموعة واسعة من الخيارات عند القيام بمهمة تحليل حركة مرور البيانات داخل الشبكة، على عكس العديد من الأدوات الاخرى، التي تقوم بمهمة التحليل مثل (Snort) و (Ossim) وعدد من (IDS/IPS)، التي تعمل علي تحذير المستخدمين ومديري الشبكات من بعض المشاكل المتعلقة بالشبكة والهجمات الأكترونية، وعلى الرغم من ذلك يحتاج محلل الشبكة عند إستخدام مثل هذه الأدوات، الي تحليل حركة مرور البيانات في الشبكة او مراقبتها اثناء وقت الذروة الخاص بالشبكة، لذلك هذه الأدوات تفتقر بشكل عام إلى المرونة في تلك الفترات على عكس محلل الحزم (Wireshark)، وبعض الأنظمة الخاصة بالمراقبة وتحليل الشبكة مثل (MARS) لها ميزة انها تنبه عن التهديدات التي من المحتمل ان تحدث للشبكة، ومع ذلك لازالت هذه الحلول ليست فعالة من حيث التكلفة لبعض المنظمات والشركات ذات الميزانيات المالية الضعيفة، والحل البديل هو استخدام برنامج لإلتقاط الحزمة المارة في الشبكة، مما يعطي فحصاً مفصلاً عن حالة الشبكة، ومثال علي هذه البرامج هو برنامج (Wireshark)، والهدف من هذه الدراسة هو جعل مسؤولي الشبكة والفنيون ادراك مزايا مراقبة الشبكة مع حزمة (Sniffer packet) مجانية ومفتوحة المصدر كأداة (Wireshark).

تعتبر عملية تحليل حركة مرور الشبكة هو إجراء روتيني، حيث تسمح لمحلل الشبكة ليس فقط من تحديد السبب الخاص بالخرق الأمني، بل يمكنه من معرفة خطوات هذا الخرق وإعادة انشاء صورة كاملة لما حدث، ولتسهيل عملية تحليل (Traffic) علي محلل الشبكة يتم استخدام برامج مخصصة لهذه العملية، ومثال علي هذه البرامج هو برنامج (Wireshark) الذي يحتوي علي واجهة رسومية ليسمح للمحلل الشبكة بالقاء نظر عامة علي (Traffic) داخل الشبكة، ولديه ايضاً القدرات الكبيرة

علي فرز الحزم الكثيرة والموجودة في الشبكة وتصفيتها، وأيضا لديه إمكانيات كثيرة في الفرز والتصفية والتحليل، وفقا لما ذكره [9]

تبين هذه الدراسة [10] انه من الممكن ان تكون انظمة المعلومات والشبكات معرضة للهجمات، حتي بعد اتخاد افضل التدابير التكنولوجية الخاصة بصد الهجمات القراصنة، مثل وضع جدار الحماية ومكافحة الفيروسات، والسبب في ذلك هو ان أمن المعلومات لايقتصر على بعض الجوانب التكنولجية فقط، ولكنه يعتمد أيضاً علي تقنيات الكشف الاخرى، التي تقدم تحليل دقيق لشبكة مثل عمليات التحليل التي تتم لي (Traffic) المارة في الشبكة، والتي قد تكشف الأختراقات التي لم يستطيع جدار الحماية والبرامج المضادة للفيروسات ان تمنعها، ويمكن لعملية تحليل الشبكة ان تكشف الهجمات والاختراقات التي قد تتجاوز جدار الحماية، حيث أن عملية التحليل مهمة في تأمين الشبكة، وينصح بأخذ محلل الحزم (Wireshark) من ضمن أدوات الحماية الخاصة بالشبكة، للحصول على بيئة امنة وبشكل متكامل قدر الامكان.

أصبحت شبكات الكمبيوتر تربط ملايين المستخدمين مع بعضهم البعض، وأصبحت شبكة البنية التحتية تؤثر على حياتنا اليومية، لذلك من المهم جداً أن تكون شبكة الكمبيوتر بحاجة الى إدارة بشكل صحيح، كما ذكرت دراسة [11]، أن إدارة الشبكة تتطلب عملية المراقبة، للحصول على أكبر قدر من الأمنية، من أجل اجتناب عمليات الأختراق بأكبر قدر ممكن.

1.2 دراسات ذات صلة Related work:

عنوان الدراسة	محتوي الدراسة
1- اداة لأتمتة منشأت (Wireshark) من اجل بروتوكول الاتصالات الملكية. (ationA Tool to Automate Gener of Wireshark Dissectors for a Proprietary Communication Protocol)	تناقش هذه الدراسة أهمية توفر نهج واضح ومتبع لمراقبة الشبكة، ويمكن التفكير في محلل الحزم (Wireshark)، الذي يعرف علي أنه برنامج مجاني ومفتوح المصدر، يستخدم لأستكشاف الأخطاء التي تحدث في الشبكة، وكذلك يعمل علي تحليل ملفات البيانات في الشبكة، كما يستخدام أيضاً في التقاط حركة مرور البيانات والبروتوكولات التي تمر عبر الشبكة، ومعرفة عمليات إرسال وإستقبال البيانات بين أجهزة الشبكة وفقا لما ذكره (Eric Golden & John W. Coffey, 2015).
2- كتاب دليل إستخدام خدمة (Wireshark) لمراقبة الشبكة (Wireshark User Guidefor Network Monitoring).	يناقش هذه الكتاب إمكانية دمج العديد من الأدوات مع بعضها البعض لبناء بيئة مراقبة شاملة تلبي كافة متطلبات الشبكة، وفقاً لما ذكره (Richard S & Ed W, 2013) يمكن التفكير في برنامج محلل حزم الشبكة (Wireshark) كجهاز قياس يمكن استخدامه للعمل مع برنامج مراقبة داخلي للشبكة للتحقق ومراقبة كافة العمليات التي تحدث في الشبكة.
3- تحليل حركة مرور الشبكة بإستخدام اداءة (Packet Sniffing): (Wireshark).	تناقش هذه الدراسة أهمية التركيز علي القيام بعملية (Sniffing) لحركة المرور (Traffic) في البيئات المختلفة للشبكة، لمساعدة مسؤولي الشبكة علي إكتشاف ضعف الشبكة بإستخدام أداة محلل الحزم (Wireshark)، هذه الأداء تمكن محلل الشبكة من تحليل (Traffic) الخاص بالشبكة والعديد من البروتوكولات مثل (IP،UDP،Tcp) وغيرها، وفقا لما ذكره (Praful Saxena & Sandeep Kumar, 2017).

الشكل(1.1) يوضح الدراسات ذات الصلة

الفصل الثالث

المتطلبات والتقنيات

1.3 متطلبات الكيان المادي (Hardware).

احد مميزات برنامج (Wireshark) انه يمكن ان يعمل على أجهزة ذات جودة تشغيل منخفضة وبفاعلية لا تختلف كثيراً عن الأجهزة ذات الجودة العالية، ولكن يفضل ان يتم تنصيبه علي أجهزة ذات جودة متوسطة او اكثر، حتى تتم عملية المراقبة والتحليل بشكل اكثر قوة وبكفاءة عالية، وتقليل الجهد والوقت، وتتلخص متطلبات المادية التي يفضل ان يكون عليها جهاز الحاسوب في الأتي:

1. جهاز حاسوب بمواصفات عالية :

- CPU:5 Core 3.00 GHz
- Memory:16 GB RAM
- Hard Disk: 4 TB

2. إذا لم نحصل على جهاز حاسوب بالمواصفات القياسية فأنه يجب ان لا تقل مواصفاته عن الأتي:

- CPU:4 Core 3.00 GHz
- Memory:4 GB RAM
- Hard Disk: 1 TB

2.3 متطلبات الكيان المعنوي (Software):

1.2.3 نظام تشغيلWindows10 .

المتطلبات الأساسية لتثبيت نظام تشغيل (Windows10) على جهاز واحد:

- CPU:4 Core 3.00 GHz
- Memory:4 GB RAM
- Hard Disk: 64 GB

2.2.3 برنامج (IPScanner).

برنامج مجاني ومفتوح المصدر، تم تصميمه ليعمل بشكل سريع وسهل الأستخدام مع منافذ (IP)، ويقوم بمسح العناوين والعديد من الأستخدامات الاخرى، ويتم استخدامه من قبل مسؤولي الشبكات والمستخدمين العاديين،وكذلك من قبل مخترقي الشبكات حول العالم، وكذلك الشركات التجارية الكبيرة والبنوك والموؤسسات الحكومية، يعمل على أكثر من نظام تشغيل مثل(Linux – Mac OS – Windows).

مميزاته :

1. مجاني ومفتوح المصدر.
2. يفحص الشبكات المحلية المرتبطة بالأنترنت.
3. فحص الملفات سواء بشكل عشوائي او محدد.
4. تصدير النتائج التي تم الحصول عليها بأكثر من تنسيق.
5. يوفر واجهة سطر الأوامر (Command-Line).
6. يعمل على أكثر من نظام تشغيل مثل (Windows)،(Mac OS)،(Linux).
7. يمكن أن يعمل دون الحاجة الي تثبيته.

3.2.3 أداة (Lipcap).

أداة تمكن مسؤول الشبكة من التقاط الحزم مثل TCP وUDP وHTTP وغيرها من البروتوكولات، بتنسيق (Lipcap) لي مستخدمي (Windows)، وتكون مستقلة عن النظام وتوفر إطاراً محمولاً لمراقبة بيانات الشبكة منخفضة المستوى.[11]

4.2.3 أداة (Winpcap).

يتم أستخدام (Winpcap) كأداة للوصول الي شبكة طبقة النقل (Link Layer)، في نظام (Windows) يسمح بالتقاط ونقل حزم الشبكة ومعرفة البروتوكولات المستخدمة، بما في ذلك تصفية الحزم على مستوى النواة (Kernel)، وتدعم أجهزة التحكم عن بعد، وتوضيح حالة الشبكة في شكل احصائيات ورسوم بيانية.]2[1

5.2.3 برنامج (Wireshark)

هو محلل حزم شبكة، مجاني ومفتوح المصدر، يمكن أستخدامه بحرية دون القلق بشأن الرسوم المدفوعة او مسألة قانونية، يستطيع محلل الشبكة بواسطته من التقاط الحزم المارة في الشبكة، ومن ثم عرض هذه البيانات وتحليلها، في سنة 1998 اطلقت اول نسخة للبرنامج بواسط المطور (Gerald Combs) تحت اسم (Ethereal)، وبعد ثمانية سنوات وبعد خلافات بينه وبين مالك حقوق البرنامج في سنة، 2006 قام (Combs) بتطوير نسخة حديثة من نفس البرنامج لكن تحت اسم (Wireshark)، في حين ان النسخة التي تحت اسم (Ethereal) بقيت علي حالها الي هذا اليوم، برنامج محلل الحزم يستخدم لفحص ما يحدث داخل الشبكة بشكل شامل مثل عمل الفولتميتر الذي يستخدمه الكهربائي لفحص ما يجري داخل كابل كهربائي، وقد زادت شعبيته بشكل كبير، وفريق التطوير الخاص به يضم الأن اكثر من 500 مساهم.1]2[

1.5.2.3 اغراض برنامج (Wireshark)

1. يستخدمه مسؤولي الشبكة لاستكشاف مشكلات الشبكة واصلاحها.
2. يستخدمه مهندسي امن الشبكة لفحص مشاكل الأمن.
3. يستخدمه المطورون لتصحيح تطبيقات بروتوكول التصحيح.1] 2[

2.5.2.3 فوائد (Wireshark):

1. دعم البروتوكولات المختلفة: يدعم (Wireshark) مجموعة واسعة من البروتوكولات مثل (TCP) و (UDP) و (HTTP) الي البروتوكولات المتقدمة مثل (AppleTalk).
2. واجهة رسومية سهلة الأستخدام: يحتوي (Wireshark) على واجهة رسومية تفاعلية تساعد في تحليل والتقاط الحزمة، كما انه يوفر العديد من الخيارات لمحلل الشبكة مثل تصفية الحزم وتصديرها.
3. التقاط (Traffic) الشبكة بشكل مباشر: يمكن (Wireshark) من التقاط البيانات الحية المتدفقة علي (Wire) وإنشاء معلومات حول نوع البروتوكولات و(Port) و(Communication channel) وما الي ذلك.

4. Open source project : (Wireshark) هو مشروع مفتوح المصدر، وقد تم تنفيذه من خلال مساهمة اكثر من 500 مطور من جميع انحاء العالم، مما يعطي حرية اكبر لي مهندسي ومحللي الشبكة من التغير في الكود الأصلي الخاص بالبرنامج على حسب احتياجات المؤسسة او الشركة التي تحتاج لإستخدام برنامج (Wireshark).[12]

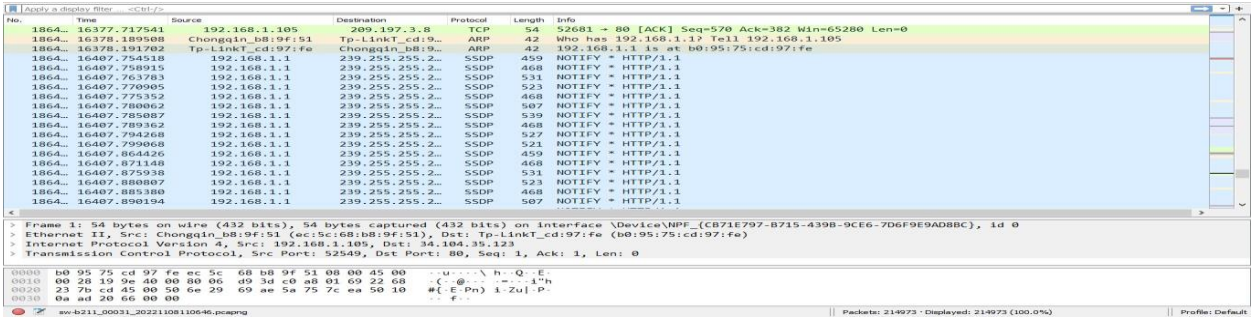
3.5.2.3 كيف يعمل (Wireshark):

يمكن تلخيص عمل (Wireshark) في عملية (Sniffing) الحزم الخاصة بالشبكة في ثلاثة خطوات:

1. Collection: ينقل (Wireshark) واجهة الشبكة الي الوضع المختلط حتي يمكن الاتقاط البيانات في شكل (binary) الأولية المتدافقة في الشبكة.
2. Conversion: يتم بعد ذلك تحويل أجزاء البيانات (binary) التي تم تجميعها الي ملف قابل للقراءة، ويتم إعادة تجميع الحزم بناءً على تسلسلها.
3. Analysis: تتضمن الخطوة الأخيرة في تحليل البيانات الملتقطة والتي تم تجميعها، حيث تتضمن عملية التحليل تحديد نوع البروتوكول والمنفذ ونوع قنوات الاتصال، وعلى مستوي متقدم في عملية التحليل، يمكن أيضاً تحليل (headers) والبروتوكولات المختلفة، لفهم متعمق لطريقة عمل الشبكة. [12]

4.5.2.3 (Wireshark GUI Panels)

تنقسم الواجهة الرسومية لبرنامج (Wireshark) الي اربعة أجزاء رئيسية :

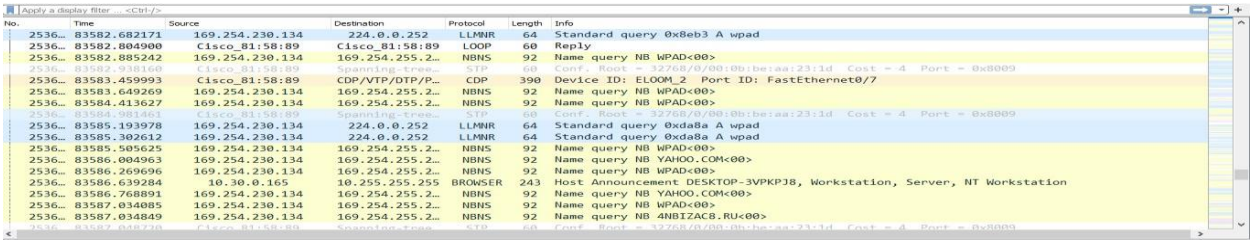


الشكل(1.3) يوضح نافذة (Wireshark GUI Panels)

1. (Capture Panel): تعرض هذه اللوحة الإلتقاط المباشر لي (Traffic) الشبكة بترتيب تسلسلي، وكل رقم في هذه اللوحة يعكس (Packet) وحيدة تم التقاطها، وتنقسم المعلومات في صفوف وأعمدة، يمثل كل صف (Packet) واحدة، ويمثل كل عمود معلومات إضافية حول (Packet).[12]

❖ تفاصيل أعمدة (Capture Panel):

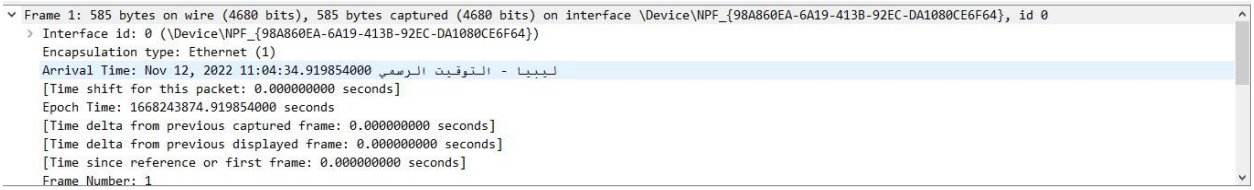
- (NO): يمثل رقم التسلسلي للحزمة لتحديد الحزم بشكل فريد.
- (Time): يمثل وقت التقاط الحزمة.
- (Source): يمثل المصدر التي تأتي منه الحزمة.
- (Destination): يمثل الوجهة التي ستذهب اليها الحزمة.
- (Protocol): يمثل نوع البروتوكول الخاص بالحزمة الملتقطة.
- (Length): يمثل حجم الحزمة.
- (Info): يمثل معلومات إضافية حول الحزمة الملتقطة.[12]



No.	Time	Source	Destination	Protocol	Length	Info
2536…	83582.682171	169.254.230.134	224.0.0.252	LLMNR	64	Standard query 0x8eb3 A wpad
2536…	83582.804900	Cisco_81:58:89	Cisco_81:58:89	LOOP	60	Reply
2536…	83582.885242	169.254.230.134	169.254.255.2…	NBNS	92	Name query NB WPAD<00>
2536…	83582.938160	Cisco_81:58:89	Spanning-tree…	STP	60	Conf. Root = 32768/0/00:0b:be:aa:23:1d Cost = 4 Port = 0x8009
2536…	83583.459993	Cisco_81:58:89	CDP/VTP/DTP/P…	CDP	390	Device ID: ELOOM_2 Port ID: FastEthernet0/7
2536…	83583.649269	169.254.230.134	169.254.255.2…	NBNS	92	Name query NB WPAD<00>
2536…	83584.413627	169.254.230.134	169.254.255.2…	NBNS	92	Name query NB WPAD<00>
2536…	83584.981061	Cisco_81:58:89	Spanning-tree…	STP	60	Conf. Root = 32768/0/00:0b:be:aa:23:1d Cost = 4 Port = 0x8009
2536…	83585.193978	169.254.230.134	224.0.0.252	LLMNR	64	Standard query 0xda8a A wpad
2536…	83585.302612	169.254.230.134	224.0.0.252	LLMNR	64	Standard query 0xda8a A wpad
2536…	83585.505625	169.254.230.134	169.254.255.2…	NBNS	92	Name query NB WPAD<00>
2536…	83586.004963	169.254.230.134	169.254.255.2…	NBNS	92	Name query NB YAHOO.COM<00>
2536…	83586.269696	169.254.230.134	169.254.255.2…	NBNS	92	Name query NB WPAD<00>
2536…	83586.639284	10.30.0.165	10.255.255.255	BROWSER	243	Host Announcement DESKTOP-3VPKPJ8, Workstation, Server, NT Workstation
2536…	83586.768891	169.254.230.134	169.254.255.2…	NBNS	92	Name query NB YAHOO.COM<00>
2536…	83587.034085	169.254.230.134	169.254.255.2…	NBNS	92	Name query NB WPAD<00>
2536…	83587.034849	169.254.230.134	169.254.255.2…	NBNS	92	Name query NB 4NBIZAC8.RU<00>
2536…	83587.038730	Cisco_81:58:89	Spanning-tree…	STP	60	Conf. Root = 32768/0/00:0b:be:aa:23:1d Cost = 4 Port = 0x8009

الشكل(2.3) يوضح نافذة (Capture Panel)

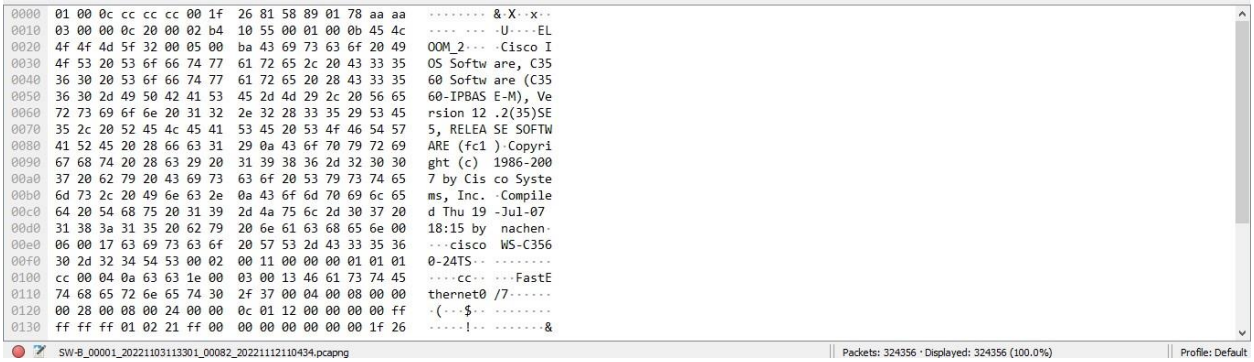
2.(Packet Details Panel): عندما يتم تحديد حزمة بيانات واحدة من واجهة الإلتقاط تكون المعلومات التفصيلية تظهر دخل لوحة (Packet Details Panel).[12]



```
Frame 1: 585 bytes on wire (4680 bits), 585 bytes captured (4680 bits) on interface \Device\NPF_{98A860EA-6A19-413B-92EC-DA1080CE6F64}, id 0
  Interface id: 0 (\Device\NPF_{98A860EA-6A19-413B-92EC-DA1080CE6F64})
  Encapsulation type: Ethernet (1)
  Arrival Time: Nov 12, 2022 11:04:34.919854000 ليبيا - التوقيت الرسمي
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1668243874.919854000 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
```

الشكل(3.3) يوضح نافذة (Packet Details Panel)

3.(Packet Bytes Panel) : تمثل هذه اللوح الحزم في شكل بايتات في ملف تفريغ، يظهر تسلسل البايت للتدفق، وتنقسم المعلومات في هذه اللوحة الي ثلاثة أعمدة، حيثُ يمثل العمود الاول (Data Offset)، والعمود التاني البيانات بشكل (hexadecimal)، والعمود الأخير يمثل (ACCII) للمعلومات.[12]



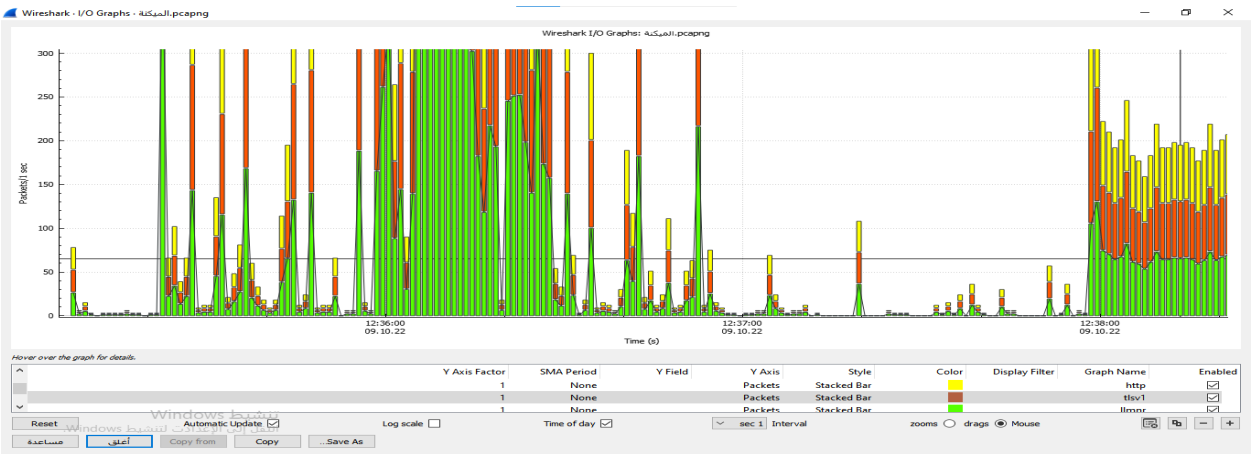
الشكل(4.3) يوضح نافذة (Packet Bytes Panel)

4.(The Status Panel): تعرض لوحة الحالة الوضع الحالي لعملية التحليل، وتوضح معلومات مثل حالة عملية الالتقاط وعدد الحزم الملتقطة، وموقع الذي تم فيه تخزين ملف الالتقاط.[11]

الشكل(5.3) يوضح نافذة (The Status Panel)

5.5.2.3 الرسوم البيانية (I/O Graphs).

الرسوم البيانية أفضل الطرق للحصول على لمحة عامة عن حالة الشبكة، وبرنامج (Wireshark) يمنح لمدير الشبكة هذه الميزة، للمساعدة في فهم وضع الشبكة التى يتم مراقبتها، لأنها تسمح بتمثيل سرعة نقل البيانات، وإمكانية العثور على طفرات وفترات ذروة الشبكة، وفترة التي تكون فيها الشبكة في أقل انتاجية، مقارنة تدفقات البيانات المتزامنة في نفس الوقت.[12]



الشكل(5.3) يوضح كيفية عمل نافذة (I/O Graphs)

6.5.2.3 مميزات برنامج (Wireshark):

1.يعمل على العديد من أنظمة التشغيل (Windows) و(Lunix).

2.التقاط الحزم بشكل مباشر من واجهة الشبكة.

3.فتح الملفات التي تحتوي على بيانات الحزمة والتي تم التقاطها باستخدام (Windump/Tcpdump)، وعدد من برامج التقاط الحزم الاخرى.

4.عرض الحزم مع معلومات البروتوكول الخاص بالحزمة بشكل مفصل.

5.حفظ بيانات الحزمة التي تم التقاطها.

6.تصدير بعض أو كل الحزم في عدد من تنسيقات ملف الألتقاط.

7.تصفية الحزم على العديد من المعايير.

8.البحث عن الحزم على العديد من المعايير.

9.عرض الحزم بشكل ملون على اساس المرشحات.

10.انشاء احصائية عن حالة الشبكة.[12]

الفصل الرابع

منهجية البحث

4 منهجية البحث Research Methodology

منهجية البحث هي مجموعة من الخطوات او المراحل المنظمة التي يتبعها الباحث لحل مشكلة معينة في نطاق البحث، بأسلوب منظم من خلال دراسة مواضيع محددة تساهم في الوصول الي نتائج ذات قيمة تساعد على حل المشكلة، وتعرف المنهجية أيضا بأنها التقنيات المستخدمة لتحديد المعلومات المتعلقة بالمشروع واختيارها ومعالجتها وتحليلها، حيث تتبع هذه الدراسة البحثية منهجية دورة حياة سيسكو (PPDIOO)، وهي منهجية تم إنتاجها من شركة (Cisco) سنة 2005 حيث تعتبر من افضل المنهجيات المستخدمة في تصميم شبكات الحاسوب (الكبيرة، المتوسطة، الصغيرة) حيث تحتوي هذه المنهجية علي (6) مراحل أساسية، تعمل على أساس دورة الحياة (The Lifecycle PPDIPP NETWORK) كالتالي (التحضير Prepare، الخطة plan، التصميم design، تنفيذ Impleent، التشغيل Operate، التحسين Optimize).[13]

1.4 مميزات المنهجية:

1. خفض تكلفة المشروع.
2. تحسين الحركة التجارية والصناعية والتعليمية حسب نوع الأستخدام.
3. سرعة الوصول الي التطبيقات والخدمات.
4. تحديد متطلبات التقنية والتحقق منها.
5. التخطيط الجيد للبنية التحتية للشبكة.
6. تصميم شبكة متكاملة ومرنة.
7. السرعة في انجاز المشاريع.
8. تخفيض مصاريف التشغيل.[13]

2.4 مراحل المنهجية.

1.مرحلة الخطة (Prepare Phase):

هي مرحلة يتم فيها التحضير الفعلي للمشروع، من حيث جمع المعلومات ومقابلة المسؤولين داخل المؤسسة، ودراسة المستندات والخرائط والفهم الجيد للشبكة، وبتالي تحديد المشاكل والأهداف الرئيسية للمشروع، كما يتم في هذه المرحلة تحديد التقنية التي سوف تستخدم في المشروع.[13]

2.مرحلة الأعداد (Plan phase):

بعد الإنتهاء من مرحلة الخطة والفهم الجيد للشبكة، تأتي بعد ذلك مرحلة الأعداد والتي تعتبر من اهم المراحل، حيث يتم فيها تحديد المتطلبات وجميع العناصر الرئيسية (hardware, software)، وبتالي يتم حل جميع المشاكل وتحقيق الأهداف المطلوبة.[12]

3.مرحلة التصميم (Design phase):

في هذه المرحلة نقوم بتصميم الشبكة الحالية داخل المؤسسة وكذالك الشبكة المتوقع إنشاؤها. [13]

4.مرحلة التنفيذ (Implement phase):

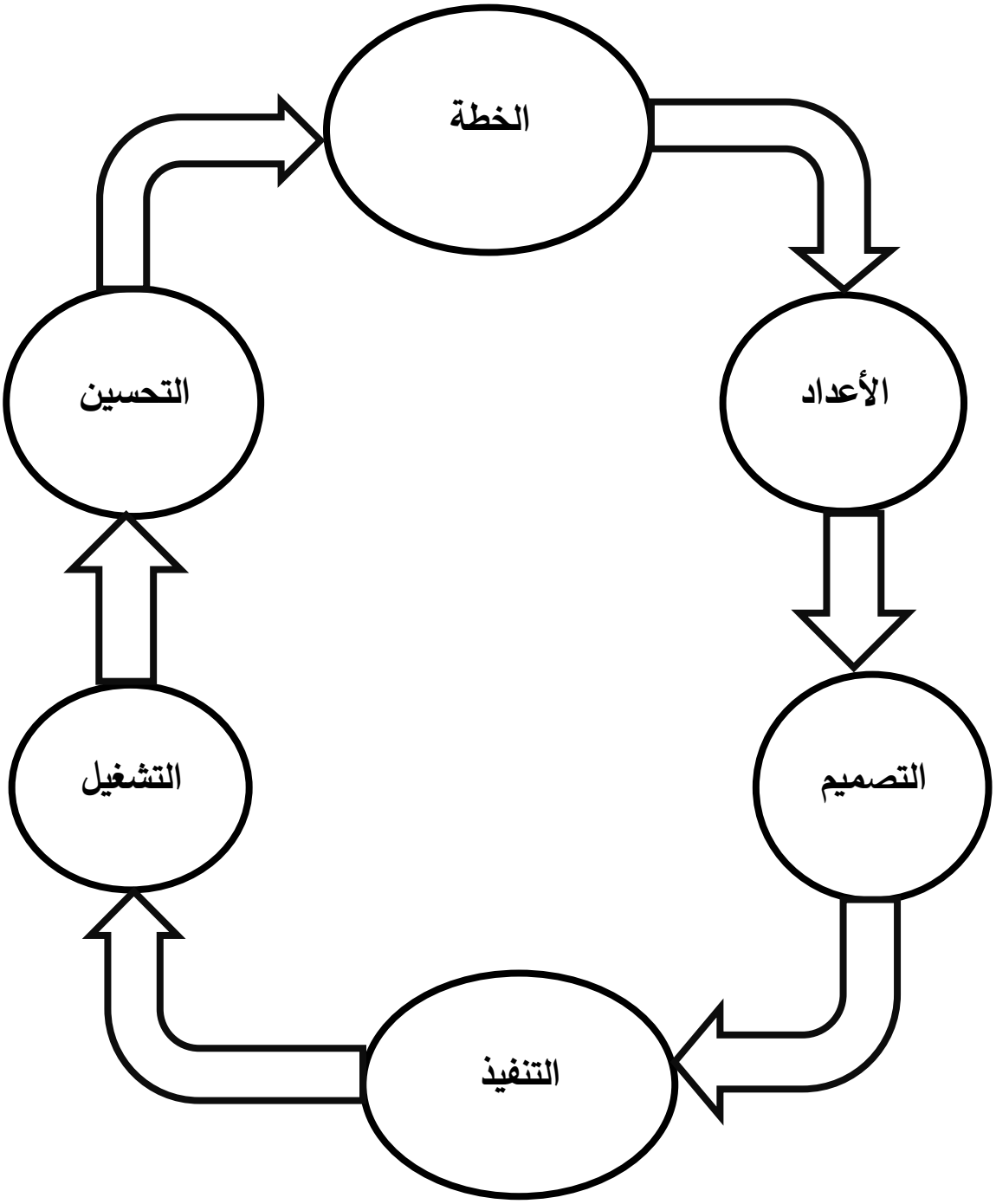
وفي هذه المرحلة يتم التطبيق الفعلي للتقنية المستخدمة، وعمل الأعدادات اللازمة للشبكة، وتطبيق الجانب العملي للمشروع.[12]

5.مرحلة التشغيل (Operate phase):

حيث يتم في هذه المرحلة التشغيل الفعلي للتقنية المستخدمة، والتأكد بأن الشبكة تعمل بشكل أكثر فاعلية.[13]

6. مرحلة التحسين (Optimize phas):

وهذه المرحلة خاصة بعمل التحسينات اللازمة للشبكة، لكي تزيد من الأداء وتواكب التطوير المستمر في عالم تقنية المعلومات، حتى تصبح الشبكة صالحة لفترات طويلة.[12]

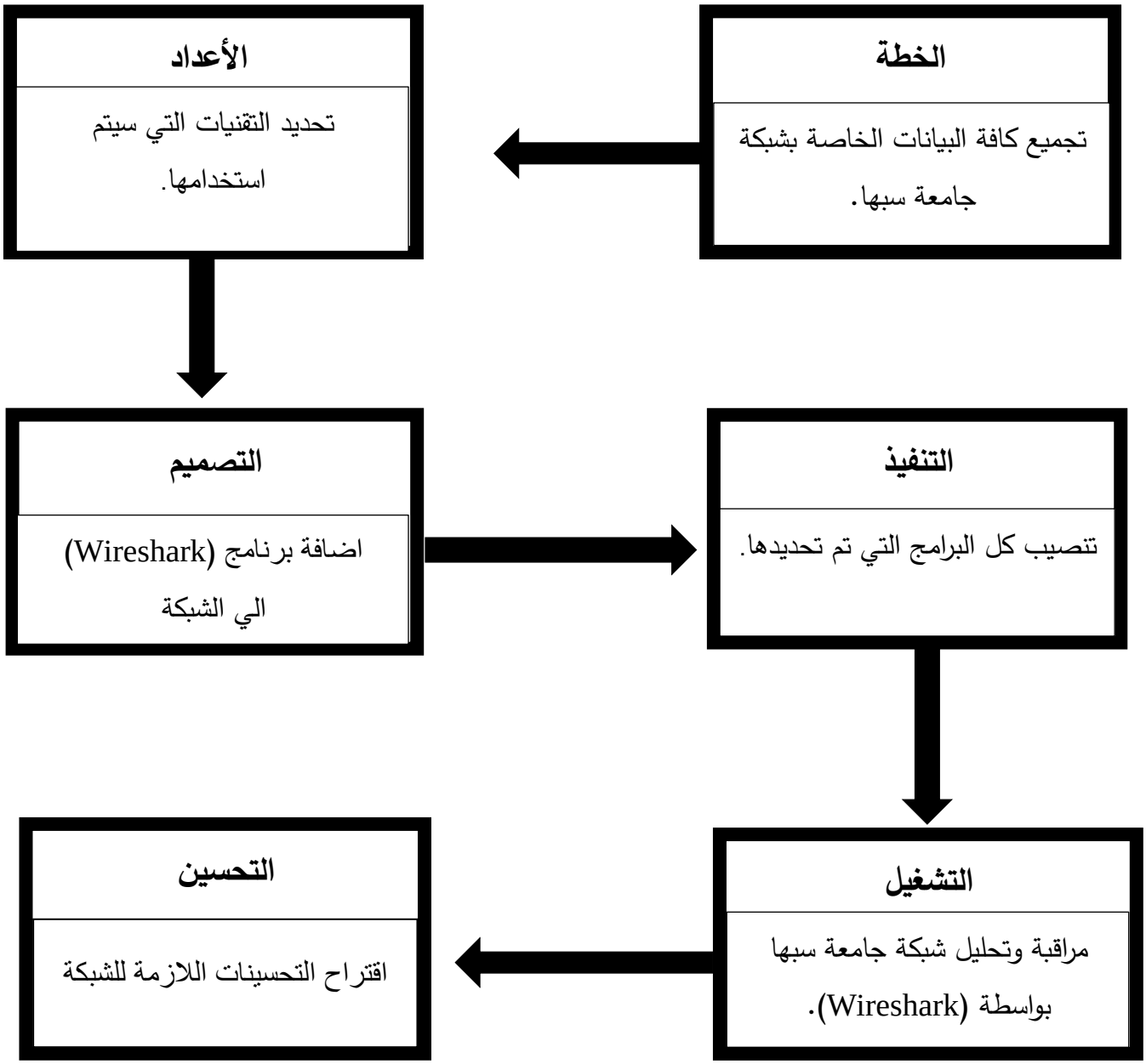


الشكل (1.4) يوضح مراحل الأساسية للمنهجية.[13]

3.4 المراحل المعتمدة في المنهجية.

تم الاعتماد في هذا المشروع على المراحل التالية:

(مرحلة الخطة ، مرحلة الأعداد ، مرحلة التصميم ، مرحلة التنفيذ ، مرحلة التشغيل ، مرحلة التحسين).



الشكل (2.4) يوضح مراحل المنهجية المعتمدة في هذا المشروع.

1. مرحلة الخطة (Prepare Phase):

حيث تم في مرحلة الخطة تجميع كافة البيانات الخاصة بشبكة جامعة سبها، إبتداءً من الوضع الحالي للشبكة والمشاكل التي تعاني منها عملية المراقبة والتحليل. وذلك من خلال إجراء مقابلة مع (مدير مركز تقنية المعلومات) ومهندسي الشبكة، تبين بعدها ان شبكة جامعة سبها تفتقد الى برامج الخاصة بالمراقبة وتحليل الشبكة، وبناء على ما تم تجميعه من بيانات، تم تحديد مشكلة الدراسة المتعلقة بالمراقبة وتحليل شبكة جامعة سبها بواسطة محلل الحزم (Wireshark)، وذلك بعد الإطلاع على العديد من الدراسات المتعلقة بهذا البرنامج، ومعرفة أهميته في عملية المراقبة التي تخص الشبكة وطريقة عمله، وكذلك تم الأطلاع ايضاً على الدراسات التي تبين أهمية تحليل ومراقبة الشبكة، ومعرفة أهمية ان تخضع الشبكة لمراقبة وتحليل بشكل دوري للحصول على نظام شبكي أمن ومستقر قدر الإمكان.

2. مرحلة الأعداد (Plan phase):

بعد الإنتهاء من مرحلة الخطة، تأتي هذه المرحلة التي تم فيها تحديد التقنيات التي يحتاجها (Wirshark)، سواء كانت تقنيات (SoftWire) او (HardWire)، وتم ايضاً دراسة المواصفات والمتطلبات التي تحتاجها كل تقنية، من أجل أن يعمل البرنامج بالصورة الصحيحة، والأستفادة من قدراته بالشكل الأفضل لتأمين شبكة جامعة سبها.

3. مرحلة التصميم (Design phase):

بعد الانتهاء من مرحلة الأعداد، تأتي هذه المرحلة التي تم فيها اعادة تصميم شبكة جامعة سبها بإضافة جهاز يحتوي على برنامج المراقبة (Wireshark).

4. مرحلة التنفيذ (Implement phase):

في هذه المرحلة تم تنصيب كل البرامج التي تم تحديدها في مرحلة الأعداد، مثل(Lipcap) و (Winpcap)، وهذه البرمجيات خاصة بعملية التقاط وتحليل حركة مرور الشبكة، وقد تم تثبيتها داخل

برنامج (Wireshark) ولكل منها مهمة معينة، وأيضاً قمنا بتنصيب نظام تشغيل التي تعمل عليه هذه البرمجيات، وتم اختيار نظام تشغيل (Windows10)، حيث ذكرنا مميزات استخدام برنامج (Wireshark) على أنه لا يقيدك بنوع معين من أنظمة التشغيل، فهو يعمل على أكثر من نظام تشغيل دون اختلاف بنفس الصورة والفاعلية مثل أنظمة تشغيل (Mac,Lunix,Windows)، ولكن تم اختيار نظام تشغيل (Windows10) بسبب أن جميع الأجهزة الخاصة بشبكة جامعة سبها تعمل بهذا النظام، وتم بعد ذلك تنصيب برنامج محلل الحزم (Wireshark) على الشبكة الخاصة بجامعة سبها.

5. مرحلة التشغيل (Operate phase):

في هذه المرحلة من المنهجية تم العمل على الأدوات التي تم تنصيبها في مرحلة التنفيذ، وتمت عملية مراقبة وتحليل شبكة جامعة سبها بواسطة محلل الشبكة (Wireshark)، ومعرفة الية عمل الشبكة والمواقع التي يتم الولوج اليها من قبل مستخدمي الشبكة، ونوع البروتوكولات التي تنقل البيانات بين المستخدمين، وكمية استهلاك (Data) في كل ساعة، حيثُ تم تنصيب (Wireshark) على احد الأجهزة الخاصة بالجامعة، والتركيز بشكل دقيق على مراقبة (Switch) الموجود في المبني (B) داخل كلية العلوم، لمدة 24 ساعة على مدار (20 يوم) بشكل متواصل، وكذلك تمت مراقبة وتحليل 4 (Routers) مقسمة بين موظفي وطلبة كلية تقنية المعلومات، وايضاً (Routers) الموجودة في مبني (مركز التطوير المعلوماتي)، وكذلك أحد (Router) الخاصة بموظفي (مركز تقنية المعلومات) خلال فترة العمل، والتي تتمثل من خلال الساعة 8 صباحاً الي الساعة 2 مساءً، وقد تم من خلال هذه المدة من معرفة كمية استهلاك البيانات الخاصة بموظفي الشبكة، ونوع البروتوكولات المستخدمة، والتأكد ما إذا كانت الشبكة تتعرض لي أي نوع من انواع الهجوم الألكتروني او اي عمليات التنصت.

6. مرحلة التحسين (Optimize phas):

وبناء على النتائج التي سيتم الوصول اليها بعد مراقبة الشبكة، سيتم ايضاً من خلالها تطبيق التحسينات المطلوبة التي تحتاجها الشبكة، من اجل الوصول الي هدف الدراسة البحثية.

الفصل الخامس

الجانب العملي

5.المقدمة

بعد الإنتهاء من مرحلة الخطة وجمع كافة البيانات الخاصة بشبكة جامعة سبها، وفقاً للمنهجية المتبعة، تأتي هذه المرحلة والتي يتم فيها التهيئة الفعلية للبيئة المراقبة والتحليل، وعمل الإعدادات اللازمة للشبكة وتطبيق كافة الجوانب العملية الخاصة بالخدمات الأساسية في المشروع، وسيتم ايضاً الحديث في هذا الباب عن ما قمنا به في الجانب العملي من الدراسة البحثية، وتنزيل البرمجيات وتنفيذ هذه البرمجيات على أرض الواقع، وأيضا كيفية السير حسب منهجية (PPDIOO).

1.5 تنصيب نظام تشغيل (Windows10).

قمنا اولاً بإختيار تنصيب نظام تشغيل (Windows10)، على الرغم من ان برنامج (Wireshark) يمكن ان يعمل على أي نظام تشغيل من الأنظمة الشائعة، سواء كانت (Windows) او (Lunix)، ولكن تم إختيار العمل علي نظام (Windows)، بسبب أن جميع الأجهزة الخاصة بالجامعة تعمل على هذا النظام، وقمنا ايضاً بتحميل نواة البرنامج على قرص تخزين (USB) ليتم تنصيبها، ويرجع السبب في ذلك الي أن تنصيب نظام التشغيل من قرص تخزين (USB) له العديد من المميزات، ولكي تصبح عملية التنصيب اكثر مرونة، بحيث يمكنك من تغيير النظام في أي وقت تريده، ويمكنك ايضاً من تنصيب النظام الذي تريده، على عكس تنصيبه بالطريقة التقليدية التي تتطلب منك قرصاً مدمجاً، ويرجع السبب الثاني لأن الجميع في وقتناً هذا تقريباً لديهم قرص تخزين (USB)، الذي يمكنهم من تحسين أداء حواسيبهم بسهولة اكثر، أو تغير النظام الخاص بحواسبهم وما الي ذلك، ولأنه أسهل وأفضل من الناحية المالية، حيثُ انه لن تحتاج لشراء قرص تخزين (USB) جديد، في حالة انه تم تنصيب نظام اخر غير النظام المطلوب، وسيتم توضيح الخطوات المذكورة بالتفصيل:

الخطوة الأولي: إعداد النظام:

في هذه الخطوة نقوم بتحضير الأنظمة والأصدرات التي نريد استخدامها، وذلك عن طريق التوجه مباشرة الي موقع الرسمي (Microsoft)، من أجل تحميل احد الأنظمة الخاصة بشركة بالصورة الرسمية.

الخطوة الثانية: قمنا بتحميل برنامج (WINtoUSB)، لأن عملية التنصيب نظام من قرص تخزين تحتاج الي برامج معينة حتى تتم بالصورة الصحيحة، وعند تنصيب البرنامج على الجهاز نقوم بعدها بفتح البرنامج، ومن ثم نقوم بإختيار النظام الذي نريد تنصيبه، ونقوم ايضاً بإختيار قرص تخزين (USB) الذي سيتم من

خلاله تنصيب النظام عليه، وبعد ذلك ننتظر حتى إنتهاء عملية التحميل حتى يصبح قرص تخزين (USB) جاهز من أجل تنصيب النظام المطلوب.

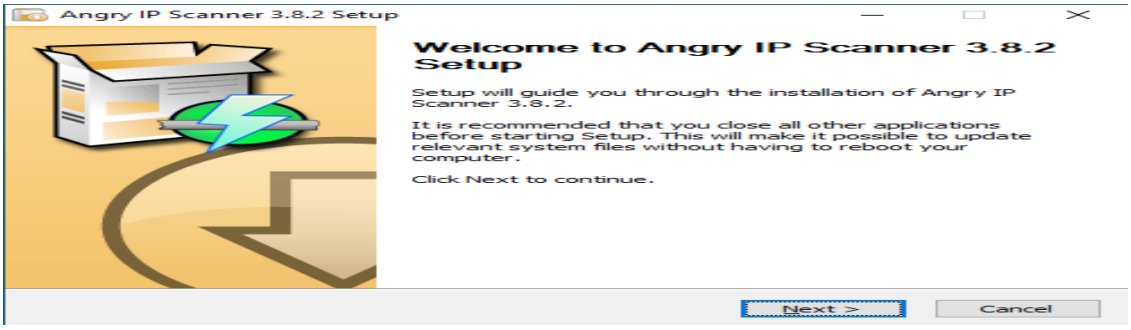
الخطوة الثالثة: نقوم بإدخال قرص تخزين (USB) في الجهاز الذي سيتم تنصيب النظام عليه، والدخول بعدها على النظام (BIOS)، والضغط على زر الذي يمكنك من تنصيب النظام الجديد، ومن ثم أتباع الإعدادات المطلوبة، حتى يتم تنصيب الجهاز بالصورة الصحيحة.

2.5 تثبيت (IP Scanner):

أولاً: نقوم بالدخول الي محرك البحث (Google) وبحث بكلمة (IPScanner Download)، ومن ثم الدخول الي الموقع الرسمي للبرنامج.

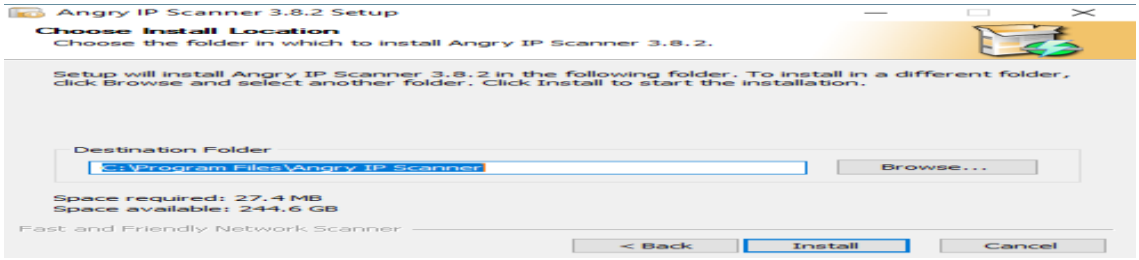
ثانياً: نقوم بعد ذلك بالذهاب الي خيار (Download) حتى يتم تنزيل احدث نسخة من برنامج (IPScanner)

ثالثاً: وبعد الإنتهاء من تنزيل كتلة البرنامج، يتم الضغط على ايقونة البرنامج لتظهر النافدة التالية:



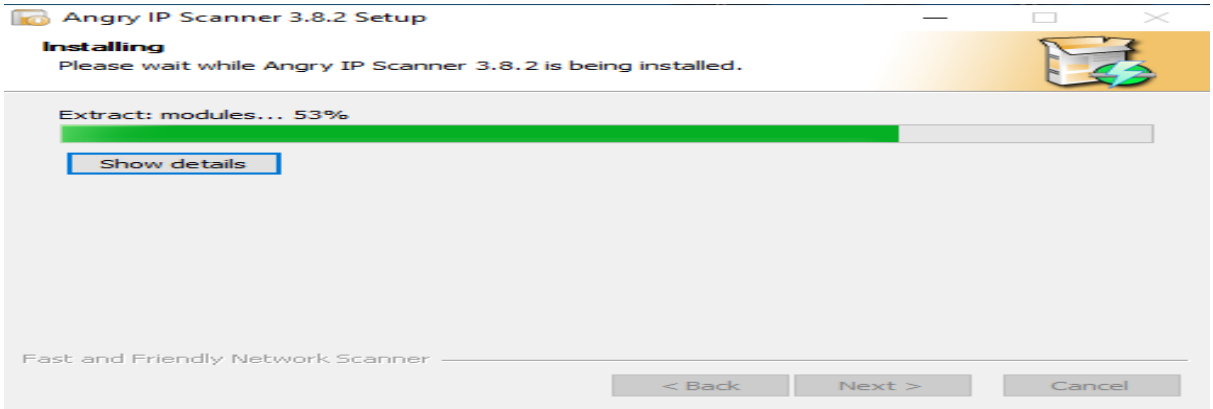
الشكل(1.5)

رابعاً: ثم نقوم بالضغط على الخيار (Next) لتظهر بعد ذلك النافدة التالية:



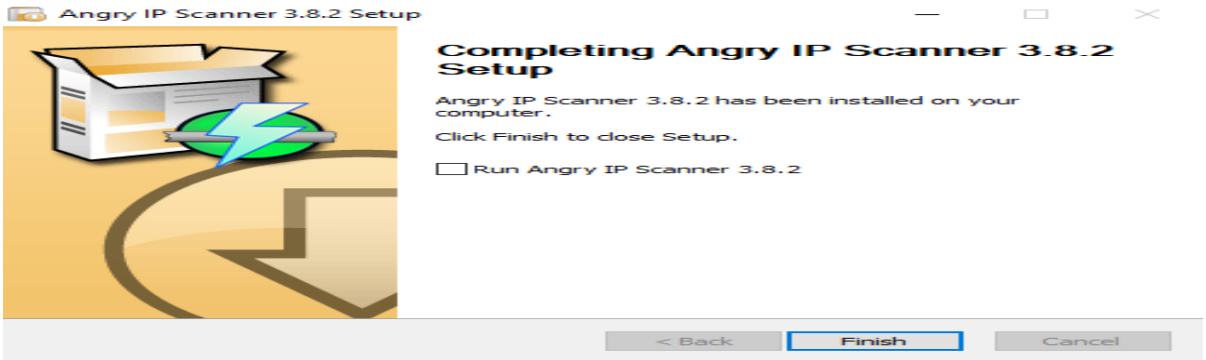
الشكل(2.5)

خامساً: بعد ذلك نقوم بضغط على الزر (Install) لتثبيت برنامج (IPScanner) بصورة النهائية كما في شكل التالي:



الشكل(3.5)

سادساً: وفي المرحلة الأخيرة من التثبيت نقوم بالضغط على خيار (Finish) لإنتهاء من مرحلة التثبيت.



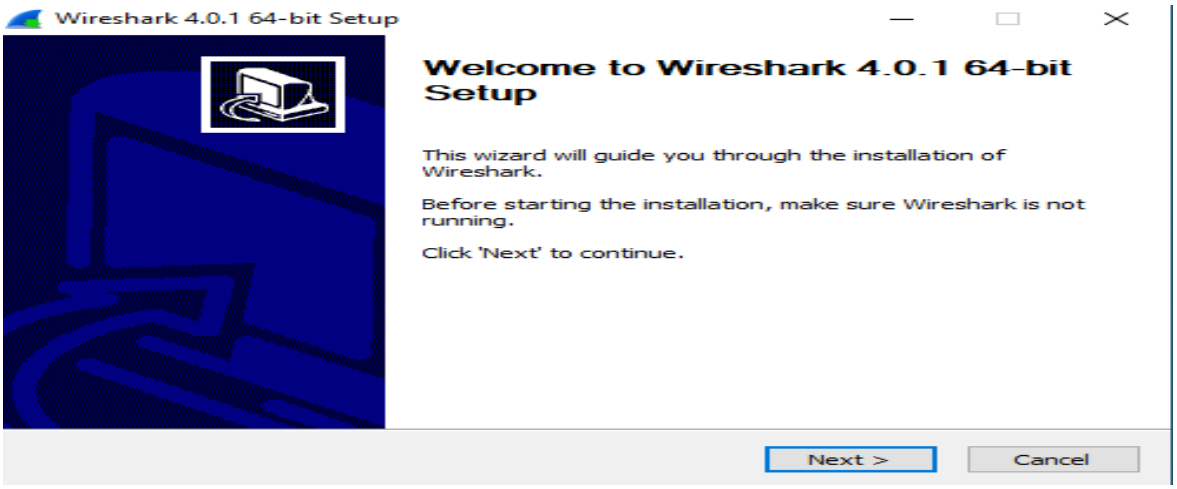
الشكل(4.5)

3.5 تثبيت برنامج (Wireshark):

الخطوة الأولى: نقوم بالذهب الي محرك بحث (Google)، ونقوم بالبحث عن كلمة (Download Wireshark) لي يظهر لنا في نتائج البحث موقع الرسمي لبرنامج محلل الحزم.

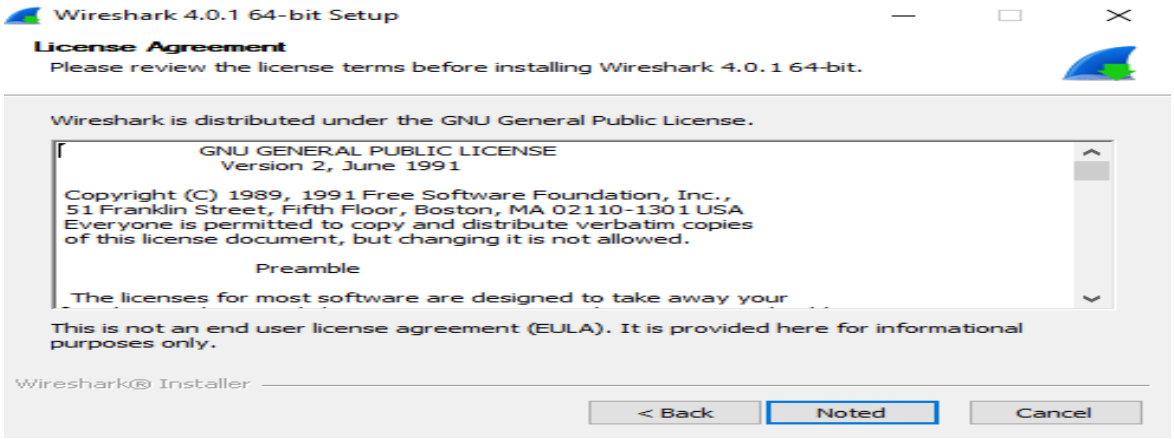
الخطوة الثانية: بعد الدخول الي موقع البرنامج والذهاب الي الصفحة التي بها كتلة البرنامج المطلوب، يضع لك الموقع الكثير من الخيارات لتنزيل البرنامج على حسب نظام الحاسوب الذي تملكه، سواء كان (64 بت) او (32 بت) وقمنا بإختيار البرنامج الذي يتناسب مع نظام (64 بت).

الخطوة الثالثة: بعد الإنتهاء من عملية التنزيل والنقر علي ايقونة البرنامج، تظهر لنا النافذة التالية ونقوم بالإختيار الخيار (Next).



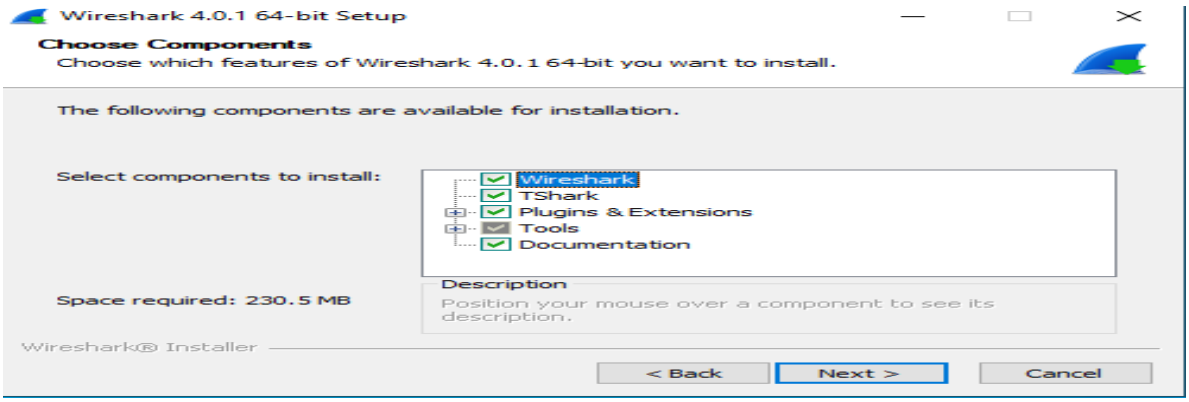
الشكل(5.5)

الخطوة الرابعة: في هذه الخطوة تظهر لك نافذة (License Agreement) التي توضح البنود القانونية لإستخدام برنامج (Wireshark) وحقوق النشر.



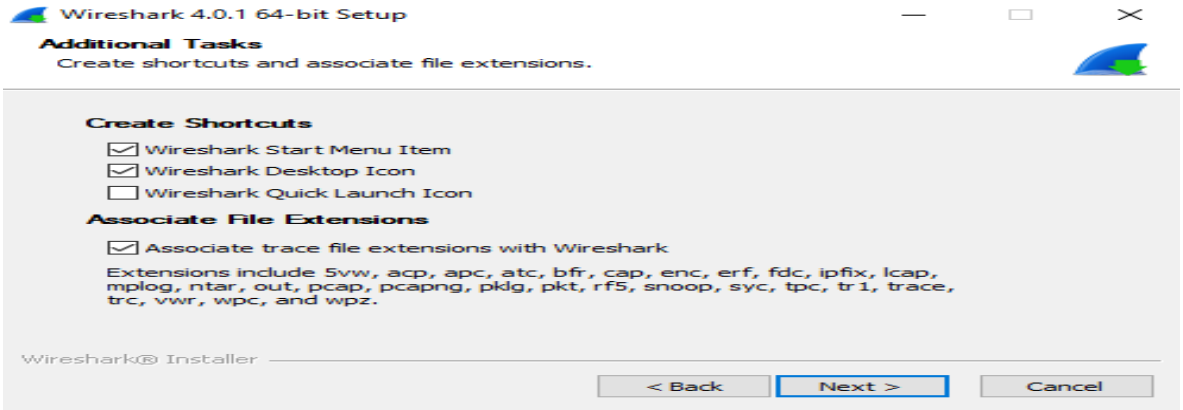
الشكل(6.5)

الخطوة الخامسة: بعد الموافقة على اتفاقية الأستخدام، نقوم بضغط على زر (Noted) لتظهر لك النافذة الخاصة بميزات الإضافية لبرنامج (Wireshark).



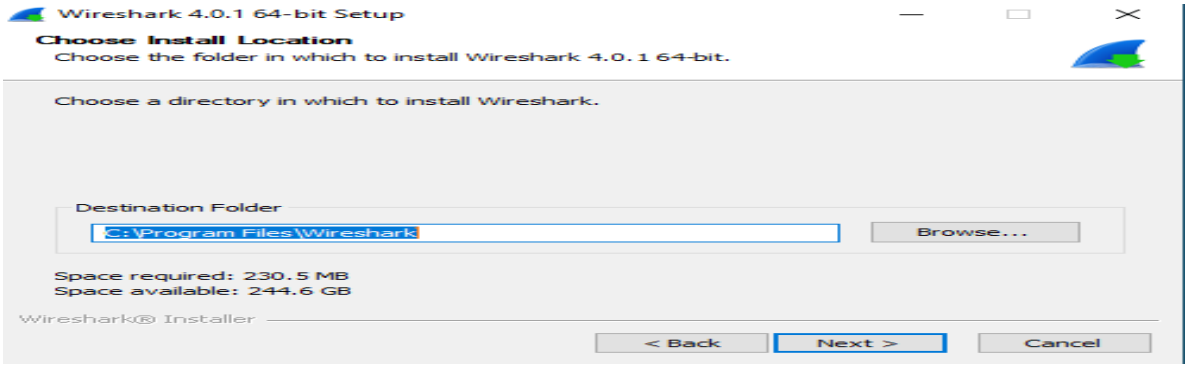
الشكل(7.5)

الخطوة السادسة: بعد الإنتهاء من أختيار الإضافات المطلوبة تظهر لك النافذة الخاصة بالإختصارات البرنامج، مثل الخيار (انشاء اختصار سطح المكتب) وجعل البرنامج ايقونة مثبتة في قائمة ابدا.



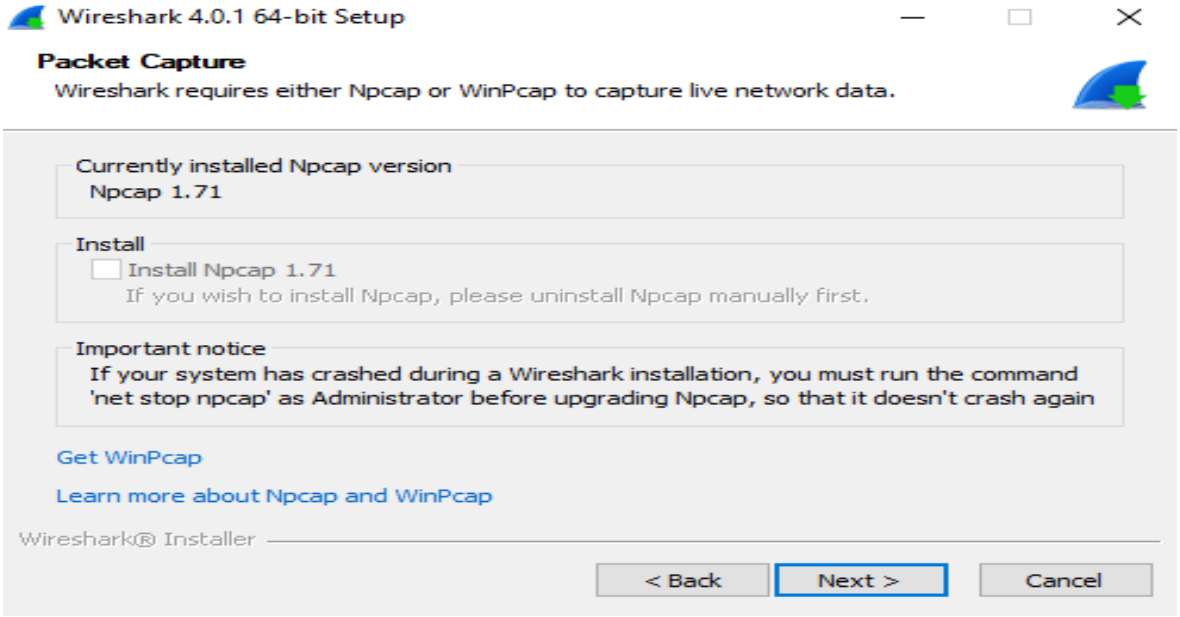
الشكل(8.5)

الخطوة السابعة: نقوم في هذه المرحلة بالإختيار الموقع الذي سيتم فيه تنزيل ملفات الخاصة بالبرنامج، والتي ستأخذ مساحة من ذاكرة الحاسوب تقدر بي 230MB فقط.



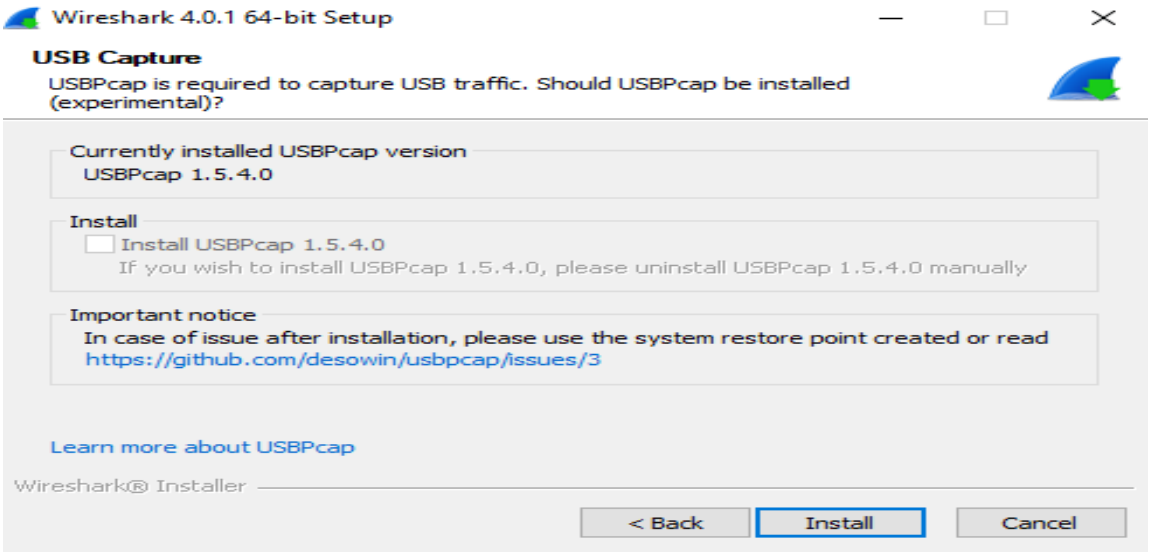
الشكل(9.5)

الخطوة الثامنة: في النسخة الأخيرة من برنامج (Wireshark) أصبح بعد ذلك تنصيب التقنيات (Lipcap) و(Winpcap) تلقائيا مع البرنامج، دون الحاجة لتثبيت كل تقنية لوحدها، حيثُ تم في هذه الخطوة من تنصيب تقنية (Npcap).



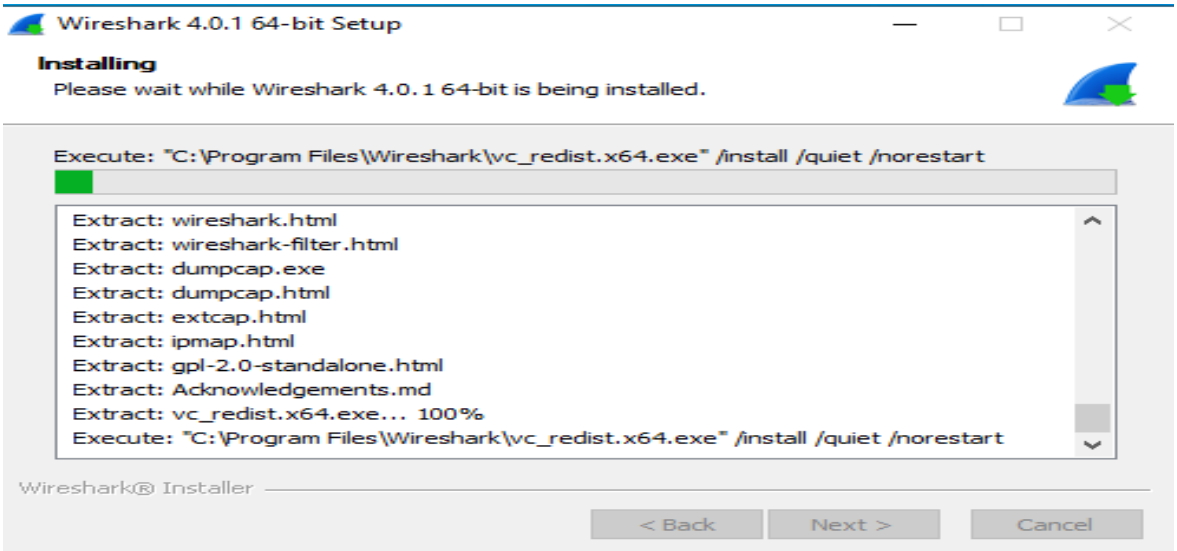
الشكل(10.5)

الخطوة التاسعة: وفي هذه الخطوة يتم تنصيب تقنية (USB Capture) الخاصة بإلتقاط مداخل (USP) الخاصة بالأجهزة المتصلة بالشبكة.



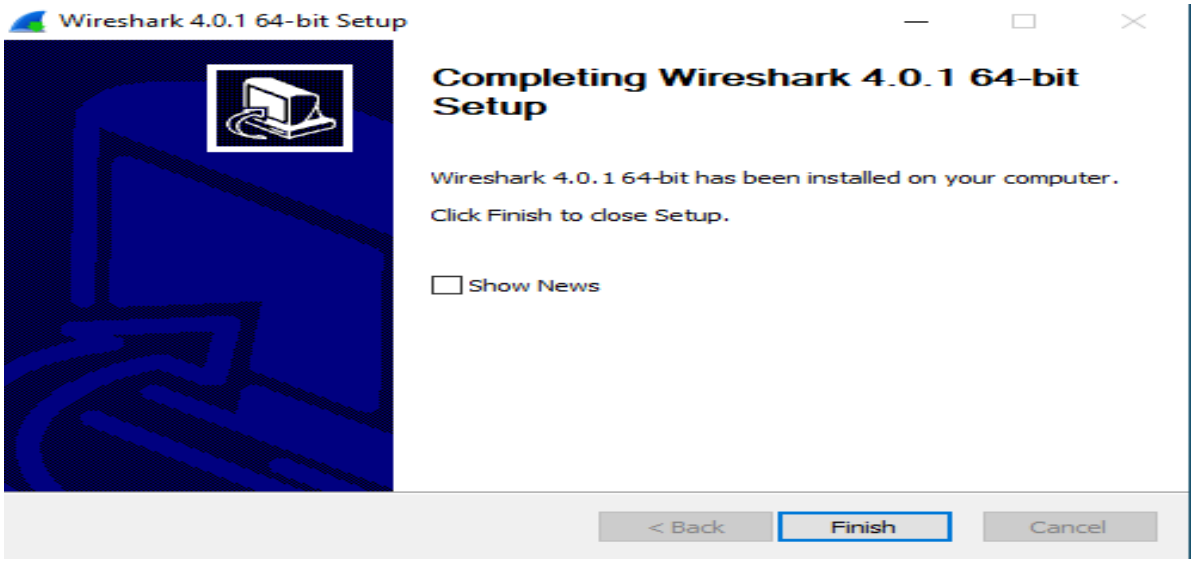
الشكل(11.5)

الخطوة العاشرة: في هذه الخطوة يتم تحميل البيانات والتقنيات (Wireshark) الخاص به.



الشكل(12.5)

الخطوة الحادي عشر: في هذه الخطوة يتم النقر على الأمر (Finish) لإنتهاء من تثبيت برنامج (Wireshark) بشكل نهائي.



الشكل(13.5)

4.5 مراقبة حركة مرور الشبكة بإستخدام (Wireshark).

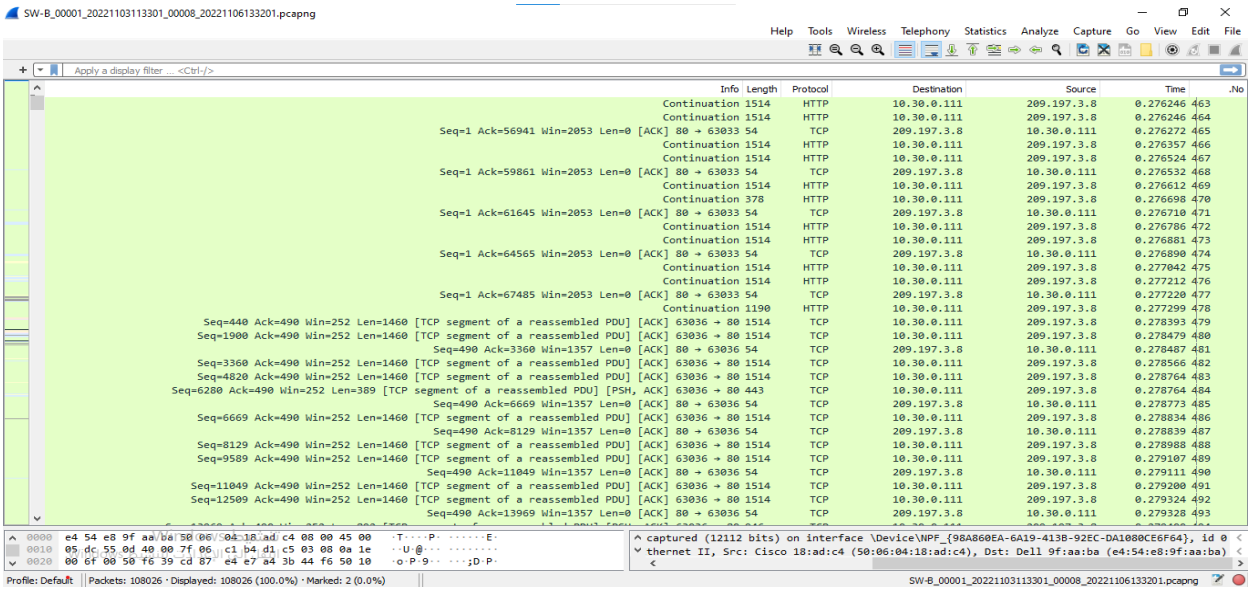
بعد الإنتهاء من تثبيت برنامج (Wireshark)، وكذلك باقي البرمجيات الجانبية التي سنحتاج اليها في عملية مراقبة وتحليل الشبكة الخاصة بجامعة سبها، تأتي بعد ذلك مرحلة تجميع البيانات من الأجهزة المتصلة بالشبكة، وقد تمت عملية التجميع من اكثر من (Switch) و(Router) الموجودة داخل الجامعة على مراحل متعددة ومنها:

1. (Switch B): يحتوي (Switch) على (port 24) الموجود في كلية العلوم بتحديد في المبنى (B)، والذي يعتبر حلقة وصل بصورة مباشرة بين مديري الأقسام والموظفين، وبين الخوادم الموجودة في مركز تقنية المعلومات.
2. ((Switch C) الاتجاه العام): يحتوي هذا (Switch) أيضا على (port 24) ويقوم بربط بين مكاتب كلية تقنية المعلومات (مكتب عميد الكلية، مكتب قسم الاتجاه العام، مكاتب أعضاء هيئة التدريس).

3. ((Switch C) قسم شبكات): يحتوي هذا (Switch) على (port 12) حيثُ انه يربط بين مكتب قسم الشبكات، ومكتب الدراسة والامتحانات، ومعامل المتواجدة في المبني C.
4. ((Switch) مركز تقنية المعلومات) يحتوي هذا (Switch) على (port 12) ويعتبر خاص بموظفي (مركز تقنية المعلومات).
5. ((tp-link) مركز التطوير المعلوماتي) يحتوي على (port 5) وهو خاص بموظفي المركز.

1.4.5 عملية مراقبة وتحليل بيانات (Switch B).

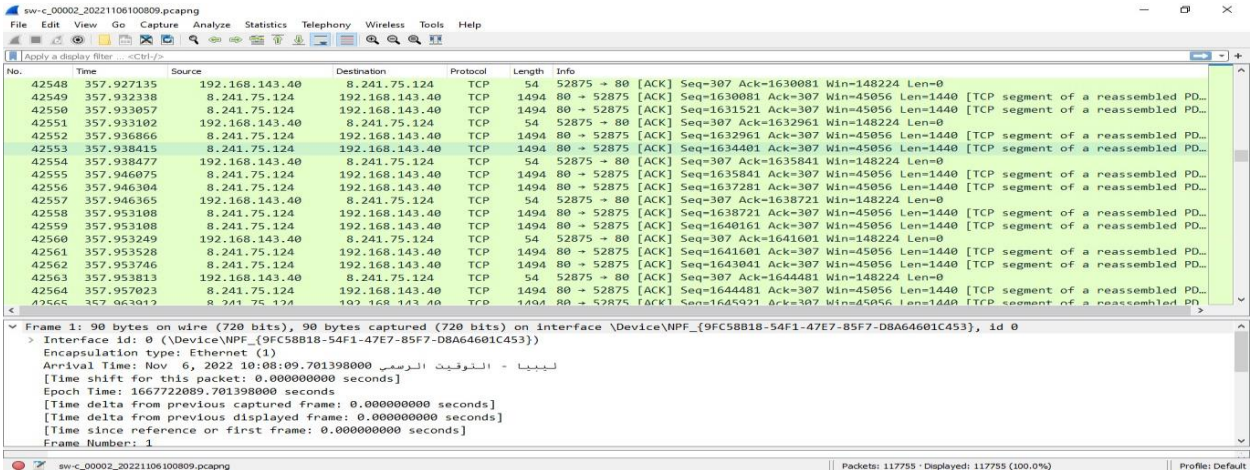
في الدراسة البحثية الخاصة بعملية المراقبة والتحليل بشبكة جامعة سبها، قمنا بالتركيز على مراقبة (Switch B) المتواجد في كلية العلوم، وذلك بعد الأطلاع على كافة فروع الجامعة، تبين بعد ذلك ان (Switch B) من اكثر (Switchs) نشاطاً، من ناحية عدد المستخدمين وحجم البيانات المستهلكة، وذلك من خلال مدة مراقبة تصل الي (20 يوم) على مدار 24 ساعة متواصلة.



الشكل(14.5) يوضح مراقبة وتحليل بيانات (Switch B).

2.4.5 مراقبة وتحليل بيانات (Switch C) الاتجاه العام.

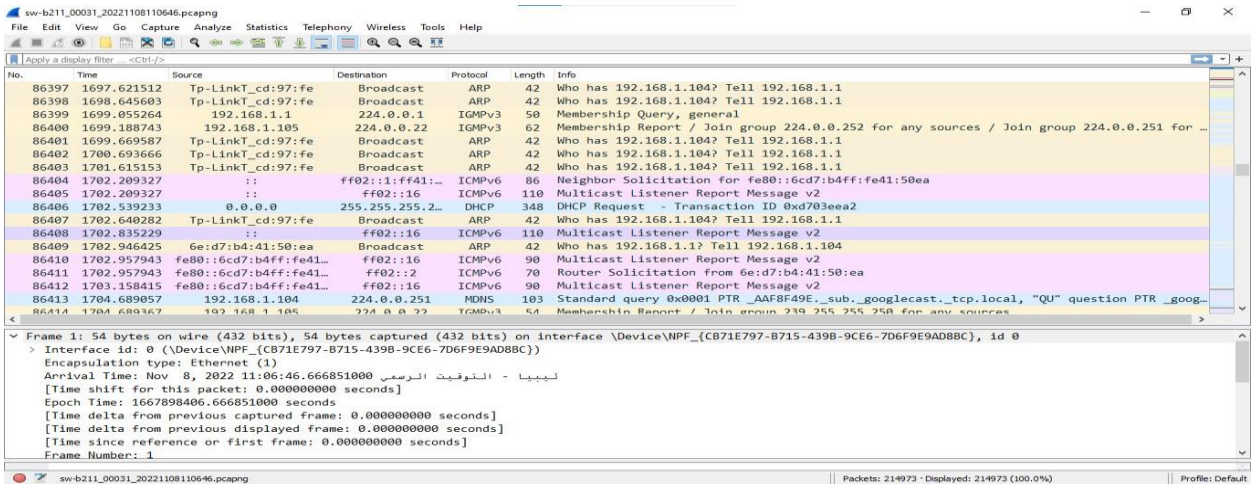
بعد ذلك قُمنا بمراقبة وتحليل (Switch) الخاص بالمبني (C) خلال فترة تصل الي (14 يوماً) في فترة الدوام الخاص بموظفي المبني.



الشكل(15.5) يوضح **مراقبة وتحليل بيانات (Switch C) الاتجاه العام**

3.4.5 مراقبة وتحليل بيانات (Switch C) قسم الشبكات.

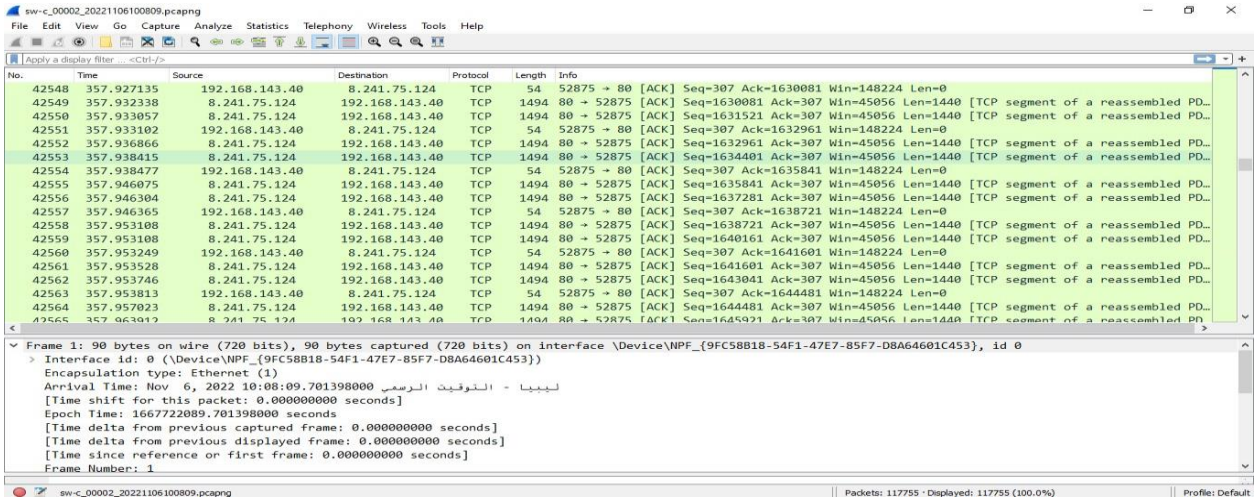
تم مراقبة وتحليل هذا (Switch) بالتوازي مع عملية المراقبة الخاصة بي (Switch) الأتجاه العام، وذلك في نفس المدة.



الشكل(16.5) يوضح مراقبة وتحليل بيانات (Switch C) قسم الشبكات

4.4.5 مراقبة وتحليل بيانات (Switch) مركز تقنية المعلومات.

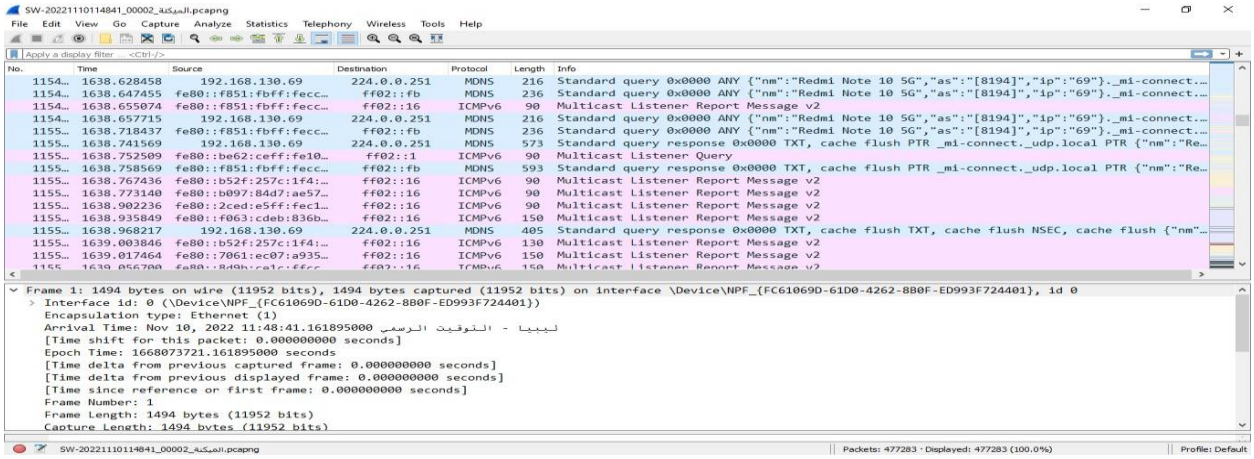
بعد الإنتهاء من عملية مراقبة وتحليل البيانات الخاصة بموظفي كلية العلوم وكلية تقنية المعلومات، تم بعدها التركيز علي (Switch) الخاص بموظفي مركز تقنية المعلومات، ودامت هذه العملية لفترة تصل الي (28) يوم على فترات متقطعة.



الشكل(17.5) يوضح مراقبة وتحليل بيانات (Switch) مركز تقنية المعلومات

5.4.5 (TP-Link) مركز التطوير المعلوماتي.

تعتبر هذه العملية من عمليات مراقبة شبكة جامعة سبها، وهي الأقصر من ناحية المدة، حيثُ انه تم مراقبة الأجهزة الخاصة بموظفي المركز لمدة (7 أيام) خلال فترات الدوام.



الشكل(18.5) يوضح مراقبة وتحليل بيانات (TP-Link) مركز التطوير المعلوماتي

الفصل السادس

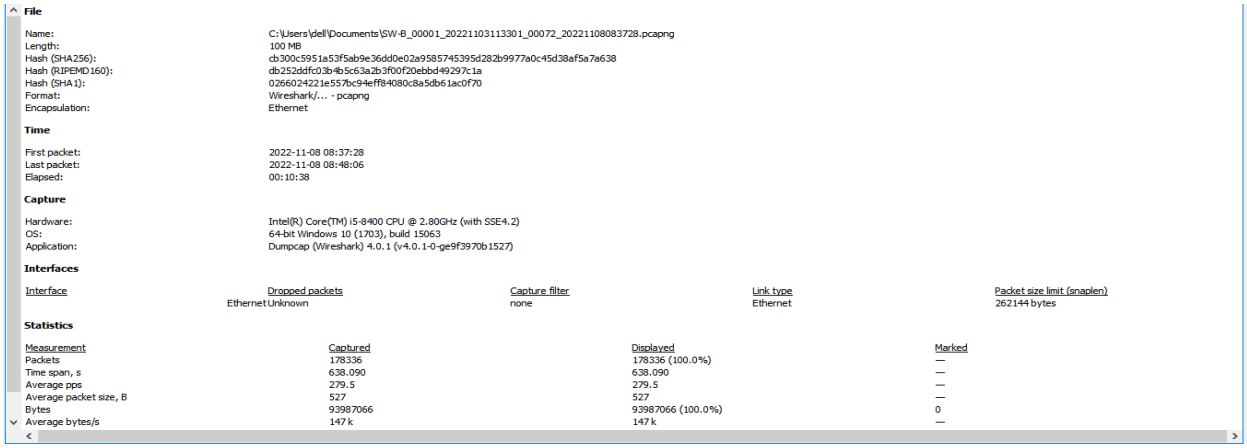
النتائج والتوصيات

1.6 النتائج والمناقشة.

بإستخدام برنامج (Wireshark) المجاني والمفتوح المصدر، تم بشكل عام مراقبة وتحليل شبكة جامعة سبها، إبتداءً من (Switch) الموجود في مركز تقنية المعلومات، و(Switch) المبني (B)، و(Switch) الموجود في مركز التطوير المعلوماتي، وكذلك ايضاً (Switchs) الموجودة في كل من قسمي الأتجاه العام وقسم الشبكات، ولضمان عمل الشبكة بشكل مستمر من دون وجود اخطاء او مشاكل أمنية، تم تهيئة خدمة المراقبة بشكل استباقي لتفادي حدوث اي عطل او اختراقات امنية قد تؤدي الي توقف الشبكة او اتلافها، وبناء على ذلك تم تنصيب برنامج (Wireshark)، الذي يوفر إمكانية مراقبة وتحليل الخدمات والموارد والأجهزة الموجودة في الشبكة، بشكل مجاني من دون وجود اي تكاليف مالية، وكذلك ايضاً يعمل على توفير كافة المعلومات حول الوضع الحالي للشبكة بشكل مفصل، وايضاً معرفة اي محاولة اختراق يمكن ان تحدث للأجهزة والخوادم المتصلة بالشبكة.

ومن الجدير بالذكر ان فاعلية مراقبة الشبكة بواسطة برنامج (Wireshark) لا تتأثر او تضعف في اوقات الذروة، فهذا البرنامج يمتاز بفاعلية وثبات طوال فترة اتصاله بالشبكة، وكذلك يوضح كافة (Traffic) الشبكة في تلك الفترة، وهذه الميزة تفتقد لها العديد من أنظمة المراقبة الأخرى، حيث انه تم تسهيل عملية المراقبة الخاصة بالشبكة، ومعرفة كل ما يحدث في الشبكة في مختلف الأوقات دون القلق من ضياع بعض البيانات، التي قد تكون مهمة لمهندس الشبكة، وترجع بالفائدة على معرفة خصائص ومشاكل الشبكة، من حيث نوع البيانات أو الكشف عن محاولات الأختراقات من قبل المخترقين الذين قد ينشطون في أوقات الذروة، حتى تقل فرص أكتشافهم أو التصدي لهم من قبل جدار الحماية، وكذلك ايضاً تمكنا من معرفة كمية البيانات الفعلية التي تم إستهلاكها في تلك الفترة، مما يعطي صورة عامة عن ماإذا كانت الشبكة بحاجة الي صيانة، أو شراء بعض المعدات الجديدة التي تغطي بعض القصور التي تتعرض لها الشبكة، سواء كانت هذه المعدات خوادم، أو اجهزة خاصة بالموظفين ومعامل الطلبة، والعمل على شراء خوادم وأجهزة ذات مواصفات عالية، من حيث حجم (RAM)، او نوعية (CPU)، حتى توفر على الموظفين الأجهزة التي تتماشى مع كمية الأستهلاك، ويضاً تسهل عليهم إكمال مهامهم في أسرع وقت وبأقل جهد، أو ان ليس هناك حاجة الي صرف مبالغ مالية في أشياء قد تكون الشبكة والمستخدمين ليسُ في حاجة لها، وتوضح النتائج التي تم التوصل اليها من خلال مراقبة الشبكة

بإستخدام (Wireshark)، الي معرفة أوقات الذروة واستهلاك الشبكة للبيانات، وتم معرفة أسباب الذروة، والتي من الممكن ان تكون اما لإستهلاك لإسباب الأستخدام الطبيعي لشبكة، او لإسباب الغير طبيعية، وتكون الأسباب الطبيعية اما لكثرة عدد الموظفين المتصلين بالشبكة بواسطة أجهزة الجامعة أثناء تأديتهم لوظائفهم، من حيث الدخول لموقع الجامعة، او عمل الأجراءات الإلكترونية الخاصة بالطلبة وأعضاء هيئة التدريس، وكان الإستهلاك في تلك الفترات لا يتجاوز (1 غيغا) في ساعة، والأسباب الغير طبيعية كانت في اوقات خارج وقت الذروة، والتي يكون فيها الإستهلاك الشبكة للبيانات مشابه لإستهلاكها في اوقات الذروة، والذي يكون بين الساعة (10 الي 1 مساءً)، وبعد ذلك تم التوصل بأن السبب في ذلك هو كثرة دخول الموظفين للمواقع التي هي خارج نطاق العمل، وكذلك ايضاً سوء إستخدام الموظفين للشبكة، مثل: (TikTok–Snapshat-Instgram)، والتي يصل فيها حجم إستهلاك الشبكة في تلك الفترة الي قرابة 3 غيغا، في مدة لا تتجاوز(30 دقيقة)، على عكس أوقات الذروة، التي يكون سببها كثرة الدخول الي موقع الجامعة، والقيام بالأعمال الجانبية مثل الدخول الي موقع (Youtube) او تصفح موقع (Facebook).



File

Name:	C:\Users\dell\Documents\SW-B_00001_20221103113301_00072_20221108083728.pcapng
Length:	100 MB
Hash (SHA256):	cb300c5951a53f5ab9e36dd0e02a9585745395d282b9977a0c45d38af5a7a638
Hash (RIPEMD160):	db252ddfc03b4b5c63a2b3f00f20ebbd49297c1a
Hash (SHA1):	0266024221e557bc94eff84080c8a5db61ac0f70
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2022-11-08 08:37:28
Last packet:	2022-11-08 08:48:06
Elapsed:	00:10:38

Capture

Hardware:	Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz (with SSE4.2)
OS:	64-bit Windows 10 (1703), build 15063
Application:	Dumpcap (Wireshark) 4.0.1 (v4.0.1-0-ge9f3970b1527)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Ethernet	Unknown	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	178336	178336 (100.0%)	—
Time span, s	638.090	638.090	—
Average pps	279.5	279.5	—
Average packet size, B	527	527	—
Bytes	93987066	93987066 (100.0%)	0
Average bytes/s	147 k	147 k	—

الشكل (1.6) يوضح حجم استهلاك البيانات

وبعد الإنتهاء من عملية تحليل (Traffic) الشبكة، وتأكد بشكل خاص من البروتوكولات التي تتواجد في الشبكة، والتركيز ايضاً على معرفة قوة معايير التشفير، والتأكد من ان الشبكة خالية من البروتوكولات التي من الممكن ان يكون بها ثغرات، قد تسبب في ضعف قوة الأمن الخاصة بالشبكة، ويوضح الجدول التالي عينات عن عملية التحليل للشبكة.

البروتوكولات التي تم التوصل إليها من (SW-B) بتاريخ 6-11-2022

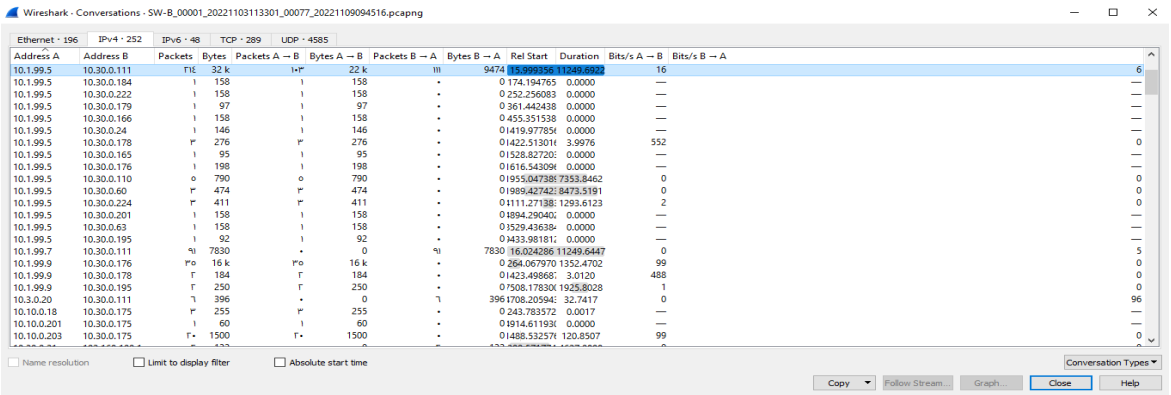
TIME	DATA	PROTOCL
10:30:08 الي 11:37:41	100MB	ARP/BROWSER/CDP/DHCPv6/LLMNR/MDNS NBNS/SSDP/STP/TCP/TLSv1/TLSv1.2/TCP/UDP
11:37:41 إلي 1:27:27	100MB	ARP/BROWSER/CDP/DHCPV6/DNS/HIP HTTP/XML/ICMP/ICMPv6/LLDP/LLMNR LOOP/MDNS/NBNS/SSDP/STP/TCP/TLSv1 TLSv1.2/UDP
1:27:27 الي 1:28:18	100MB	ARP/DHCPv6/DNS/HTTP/ICMP/LLMNR/LOOP MBNS/SSDP/SSL/STP/TCP/TLSv1.2
1:28:18 الي 1:28:54	100MB	ARP/DNS/HTTP/ICMP/LLMNR/MDNS/NBNS SSDP/STP/TCP
1:28:54 الي 1:29:26	100MB	ARP/DNS/HTTP/ICMP/LLMNR/LOOP/MDNS NBNS/SSDP/STP/TCP/TLSv1
1:29:26 الي 1:30:02	100MB	ARP/DNS/HTTP/ICMPv6/LLMNR/LOOP/MDNS NBNS/SSDP/STP/TCP/UDP
1:30:02 الي 1:30:38	100MB	ARP/DNS/HTTP/ICMP/LLMNR/LOOP/MDNS/NBNS SSDP/STP/TCP

الشكل(2.6) يوضح نتائج عينة لبعض عمليات التحليل

وهذه النتائج التي تم التوصل اليها، توضح أن شبكة جامعة سبها، يوجد بيها بعض القصور في الجانب الأمني، من حيث نوع البروتوكولات المتواجدة داخل الشبكة، فالبعض من هذه البروتكولات يكون استخدامها غير أمن مثل بروتوكول (HTTP)، الذي لا يوفر اي خيار عن تشفير البيانات الخاصة بالمستخدم، والذي يستعمل في المواقع الغير موثوقة او المزيفة، والتي تم تصميمها من قبل بعض

المخترقين، حيث تقوم بإستغلال قلة معرفة بعض مستخدمي الشبكة بكيفية التصفح الأمن، ووجدنا ايضاً بعض البروتوكولات التي بها ثغرات، والتي قد تم التوقف عن إصدار تحديثات لها، لتغطي هذه الثغرات مثل بروتوكول (LLMNR)، والتي أوقفت شركة مايكروسوفت عن إصدار التحديثات الخاصة به، وكذلك عدم التوقف عن إستعمال بعض البروتوكولات القديمة، والتي يوجد لها إصدار أحدث وأفضل من الناحية الأمنية وسرعة وصولها للبيانات مثل بروتوكول (TLSv1)، والأصدار الثاني له (TLSv1.2)، والذي يعتبران من أقدم بروتوكولات تأمين البيانات، وكما اعلنت العديد من شركات الأنترنت والحواسيب الكبرى مثل (Microsoft/Apple/Google/Mozilla)، عن إيقاف الدعم عن البروتوكولات المذكورة في مواقعهم ومتصفحاتهم في عام (2020 و 2021)، وبناءً على ذلك يجب تحديث الخوادم والأجهزة والمواقع الخاصة بجامعة سبها، وكذلك العمل على إيقاف البروتوكولات القديمة، التي تم إيقاف دعمها من قبل الشركات العالمية، والتي يوجد بها ثغرات، لتصبح الشبكة مواكبة للتطور المستمر في علم تشفير البينات، والحصول علي شبكة أمنة وخالي بأكبر قدر ممكن من الثغرات.

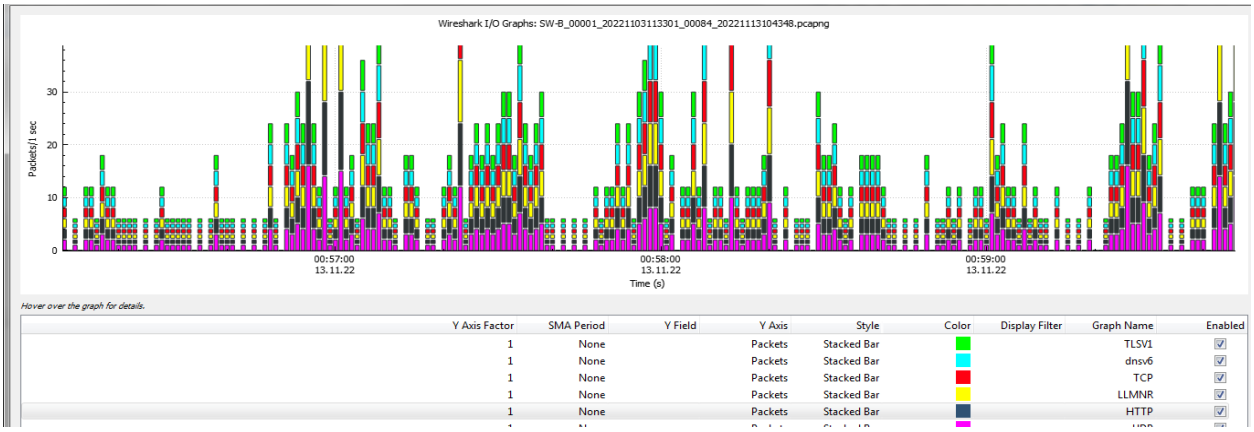
وتمكنا كذلك من معرفة (Source) و (Destination) الخاصة بالبيانات، وذلك للتأكد من أن الشبكة لا يوجد بها اي عملية اختراق في الأجهزة الخاصة بالموظفين من قبل احد القراصنة، ويتم اكتشاف هذه العملية، عندما يقوم المخترق بالدخول الي احد أجهزة الشبكة، ومحاولة إرسال البيانات إليه، نتمكن في تلك الحالة من معرفة عنوان (IP)، الذي يحاول المخترق إرسال البيانات اليه، فيمكن أكتشافه بواسطة برنامج (Wireshark)، بالدخول الي تقنية (Conversation)، ليتم بعدها تتبع مصادر إرسال البيانات، وإيقاف مثل هذه الهجمات قبل ان تحدث وفي أسرع وقت، لتجنب أكبر قدر ممكن من الخسائر في البيانات الحساسة، وتجنب ايضاً عمليات الأبتزاز الإلكتروني.



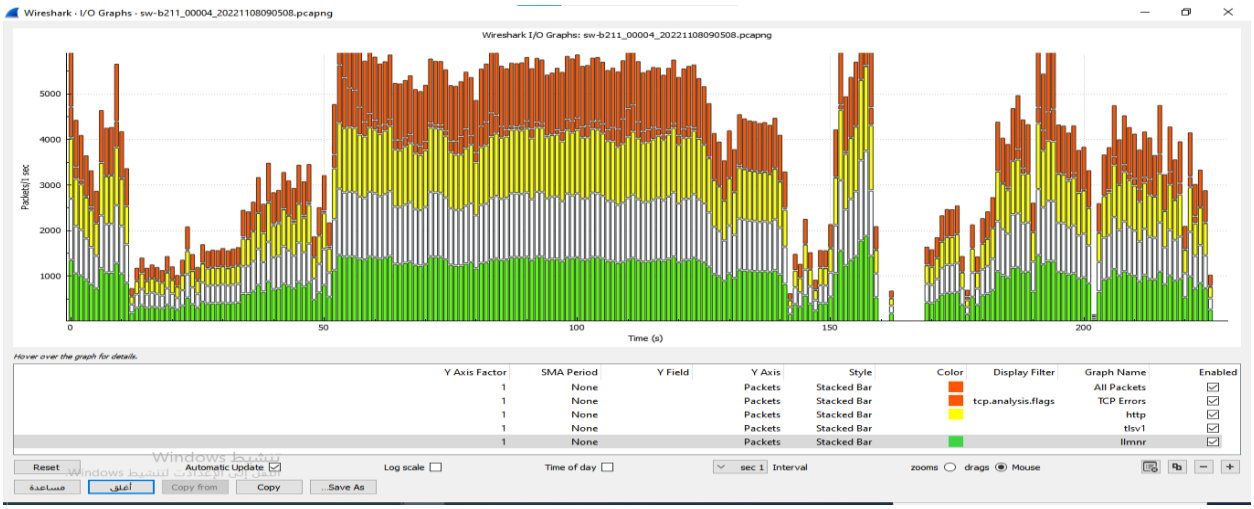
الشكل(3.6) يوضح (Source) و(Destination) البيانات بين المستخدمين.

2.6 نتائج تحليل الشبكة:

بعد ان تم تحليل كل من (Switchs) والأجهزة الخاصة بشبكة جامعة سبها، بإستخدام برنامج (Wireshark)، تقوم المستشعرات (I\O Graph) الخاصة بهذا البرنامج بعرض كافة البروتوكولات والمعلومات التي تحدث في الشبكة لكل الأجهزة المتصلة بالشبكة، وتخزينها في قاعدة بيانات البرنامج، وتنتج من خلال هذه المعلومات رسوم بيانية وخرائط توضح المعدل الطبيعي للبروتوكولات الموجودة في الشبكة.

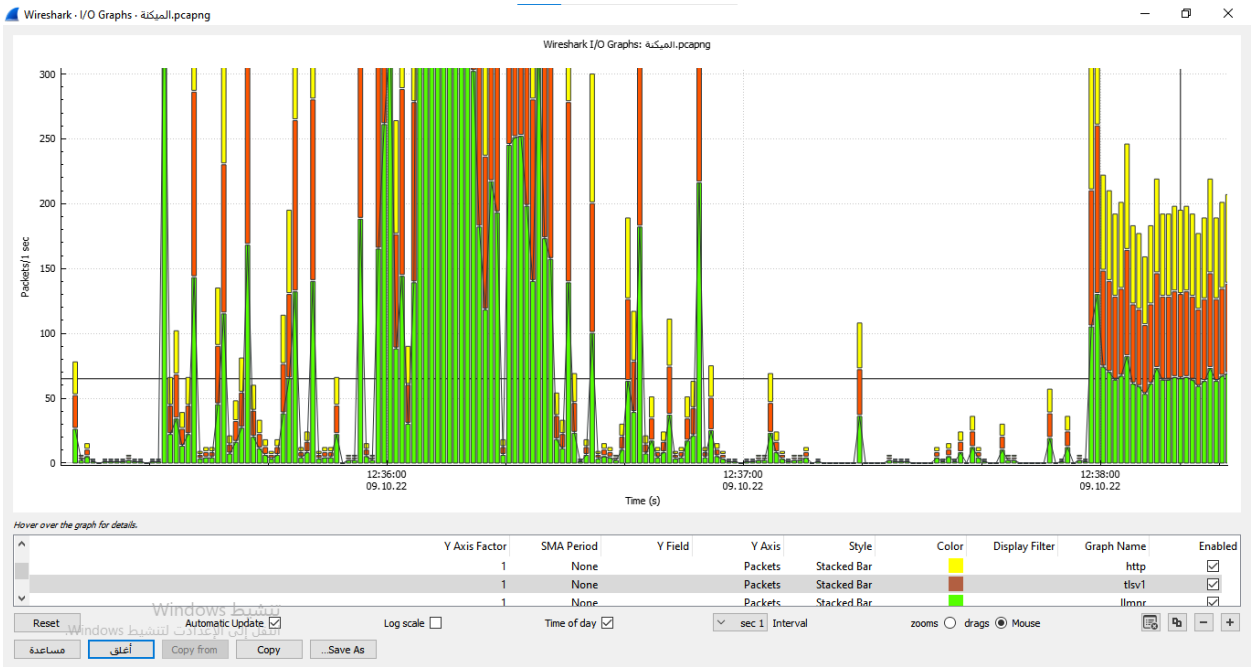


شكل (4.6) يوضح معدل حركة البروتوكولات الخاصة بي (Switch-B).

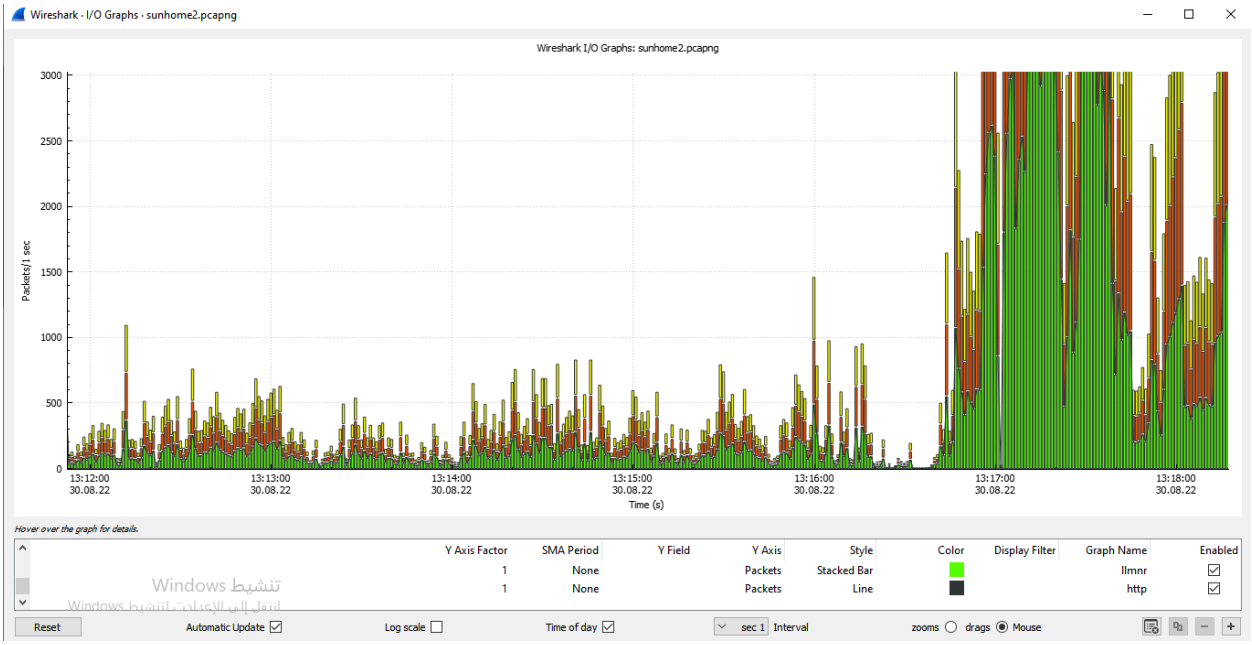


شكل (5.6) يوضح معدل حركة البروتوكولات الخاصة بي (Switch-C).

شكل (6.6) يوضح معدل حركة البروتوكولات الخاصة بي (Switch-C – الاتجاه العام).



شكل (7.6) يوضح معدل حركة البروتوكولات الخاصة بي (Switch – مركز تطوير المعلوماتي).



شكل (8.6) يوضح معدل حركة البروتوكولات الخاصة بي (Switch – مركز تقنية المعلومات).

كما نلاحظ في الرسوم البيانية التي تنتجها اداة (I\O Graph)، والتي تعطي صور عن حالة كل بروتوكول داخل الشبكة، وتمثيل (Traffic) الخاص بالشبكة، وبشكل يسهل من معرفة وقت استخدام كل بروتوكول، ومعرفة ايضاً (IP) الجهاز الذي يستخدمه، مما يسهل على مديري الشبكة معرفة خصائص الشبكة التي يديرها، ونوع الأجراءات والحلول التي من الممكن إتخاذها في بعض المشاكل التي من الممكن ان تحدث.

3.6 العوائق والصعوبات:

1. قلة امكانيات توفير اجهزة بالمواصفات التي تحتاجها الشبكة، اثناء عملية المراقبة لتعمل الشبكة بأداء جيد.

4.6 التوصيات:

تتلخص توصيات الدراسة في الخطوات التالية:

1. تطبيق برنامج المراقبة (Wireshark) على شبكة جامعة سبها.
2. استخدام او تطبيق اكثر من نوع من برامج المراقبة على الشبكة.
3. وضع حصة محدودة لكمية استهلاك البيانات من قبل الموظفين، عند استخدامهم لشبكة الجامعة من اجهزتهم الشخصية، لترشيد وتقليل من الاستهلاك الغير مفيد للإنترنت.

5.6 الخلاصة Conclusion

تم في هذه الدراسة تنصيب برنامج (Wireshark)، وإعداد كافة الخدمات المطلوبة على نظام (Windows)، وذلك لغرض توفير الحلول لكافة المشاكل المتعلقة بعملية المراقبة التي تعاني منها شبكة جامعة سبها، والتي تم التوصل اليها بعد إجراء مقابلة مع مدير (مركز تقنية المعلومات)، ومعرفة بعدها بأن شبكة جامعة سبها تعاني من عدم وجود اي برنامج مراقبة، وبعد توفير برنامج المراقبة المجاني والمفتوح المصدر للشبكة، قمنا بعدها بواسطة هذا البرنامج من القيام بعملية مراقبة لشبكة الجامعة، ومن خلال عملية المراقبة تم إكتشاف العديد من البروتوكولات التي يوجد بها ثغرات، والتي قد تسبب في ضعف الجانب الأمني لشبكة، ومن هذه البروتوكولات (LLMNR-TLSV1-TLSV1.2-HTTP)، وتم بعد ذلك معرفة خصائص الشبكة، من حيث كمية البيانات المستهلكة ووقت الذروة، التي تكون فيه الشبكة في قمة إستهلاكها للبيانات، وتم ايضاً تمثيل هذه الخصائص على هيئة نماذج رسومية، وكذلك المسار الذي تعبر من خلاله البيانات، وقمنا ايضاً بمعرفة المواقع التي يتم الدخول إليها من قبل المستخدمين، ومدى أمن هذه المواقع، والتأكد من عدم الدخول على المواقع المزيفة، التي يمكن أن تسبب في أختراقات لبيانات المستخدمين، ويجب توفير هذا البرنامج من قبل مهندس الشبكة، لمساعدته في تحليل ومراقبة الشبكة، ومعرفة كافة خصائصها، وذلك من دون وجود اي تكاليف مالية.

References المراجع

1. Muhamed Alfawareh(2015)A deeper Look into Network Traffic Analysis Using Wireshark.
2. Najd Muhaed(2019)Snort Implement With Wireshark Helping DDos Attack in The cloud Compting.
3. Febrian Rusdi & Sazilah Salam (2018) Malware Detection.
4. Praful Saxen & Sandeep Kumar Sharma (2017) Analysis of Network Traffic by using Packet Sniffing Tool: Wireshark.
5. Richard s & Ed w.2013
6. Eric Golden & John W. Coffey(2015) A Tool to Automate Generation of Wireshark Dissectors for a Proprietary Communication Protocol.
7. Haroon Iqbal & Sameena Naaz (2019) Wireshark as a Tool for Detection of Various LAN Attacks.
8. Ghilam Biswas & Ashutosh(2014) An Insight in to Network Traffic Analysis using Packet Sniffer.
9. Igor Kotenko1;2∗, Maxim Kolomeets1;2, Andrey Chechulin1;2, and Yannick Chevalier2 (2018) A visual analytics approach for the cyber forensics based on different views of the network traffic.
10. Mustapha Adamu Mohammed*, Ashigbi Franlin Degadzor, Botchey Francis Effrim, Kwame Anim Appiah (2017) BRUTE FORCE ATTACK DETECTION AND PREVENTION ON A NETWORK USING WIRESHARK ANALYSIS.
11. Jakub Svoboda, Ibrahim Ghfir, Vaclavr Presonal(2018) Network Montring Approaches:An Overview
12. Chris Sanders(2011)Practical Packet Analysis.
13. عبدالسلام صالح الراشدي، وليد علي البريكي (2018)منهجية دورة حياة سيسكو

الملاحق

(Appendix 1)

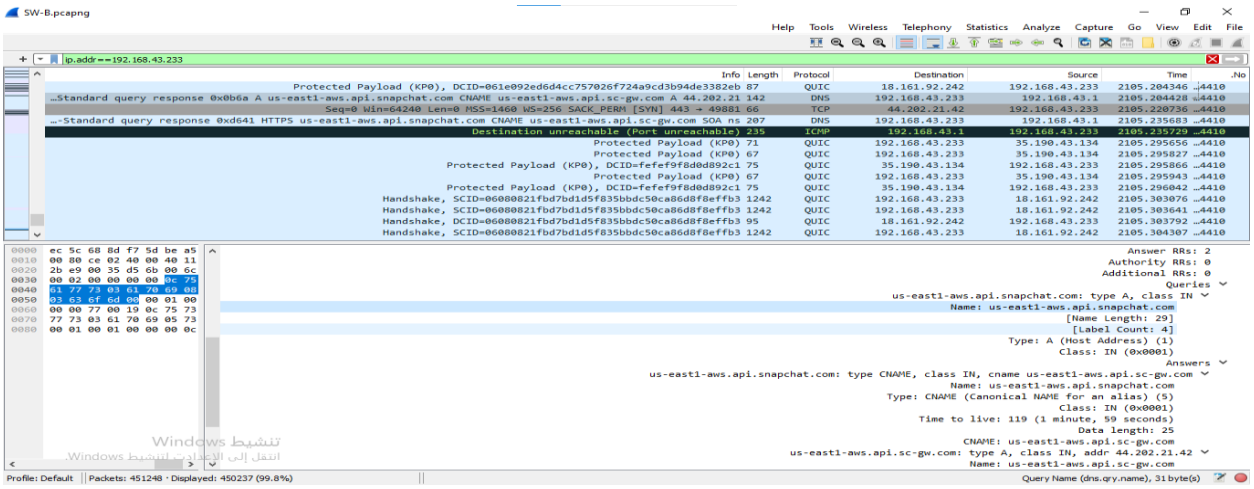
تصميم البحث Research Design

التصميم هو عبارة عن إطار من الأساليب وطرق البحث التي إختارها الباحث ليحقق أهداف دراسته، والشكل التالي يوضح تصميم البحث لدراسة المقترحة

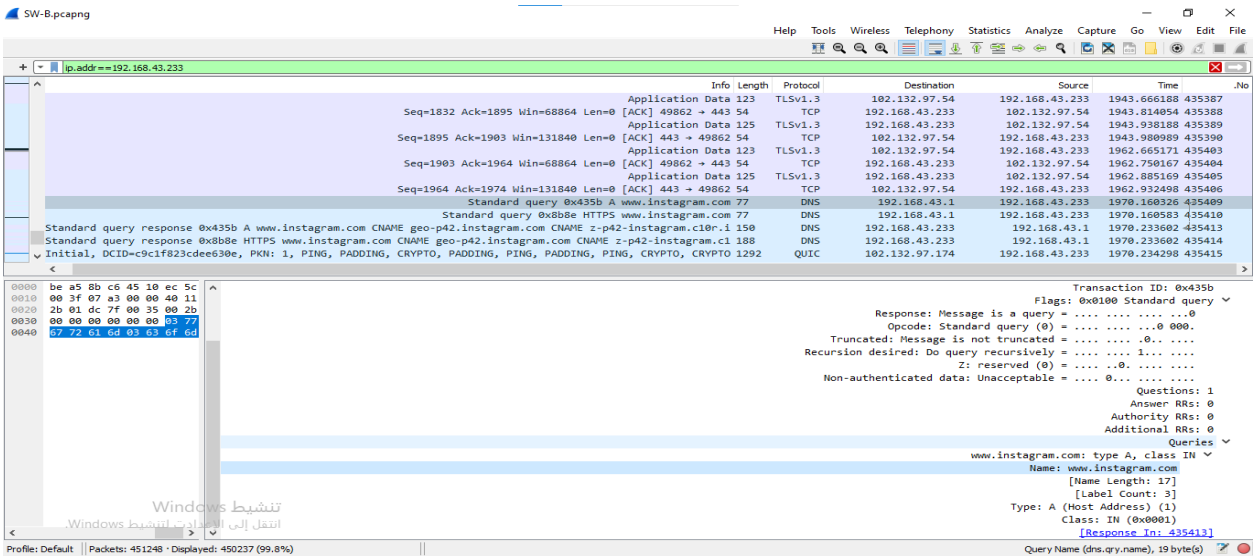
الدراسات السابقة	– تحديد الدراسات المتعلقة بالتحديات التي تواجه مراقبة شبكات الحاسوب. – استخراج الفجوة المعرفية من الدراسات المتعلقة الأقرب لدراسة المقترحة.
تحديد المشكلة	– لايوجد نهج واضح ومتبع لمراقبة وتحليل الشبكة بشكل كامل. – عدم التأكد من ان كافة البروتوكولات التي تتواجد في الشبكة بأنها خالية من الثغرات.
المتطلبات	– برنامج مراقبة واجهزة لتنفيذ نظام التشغيل الذي سيتم عليه تنفيذ النظام المقترح.
منهجية البحث	– استخدام منهجية دورة حياة سيسكو (PPDIOO) لنظام المقترح بعد تفيذه على الشبكة وتحليل النتائج المتحصل عليها وذلك لغرض الحصول على نظام المراقبة الأنسب لمراقبة بيئة الشبكة.
تنفيذ النظام	– تنفيذ نظام المراقبة (Wireshark) للتطوير نظام مراقبة شامل للشبكة الحالية .
النتائج المتوقعة	– تسهيل عملية تحليل ومراقبة شبكة جامعة سبها. – معرفة انواع البروتوكولات المستخدمة والتأكد من انها أمنة. – معرفة اوقات الذروة الخاصة بالشبكة.
التحقق من النتائج	– تحليل ومناقشة النتائج التي تم الحصول عليها ومقارنتها مع الأهداف المقترحة لحل المشكلة وتحديد في حال توافقت معها او لا.
كتابة التتقارير	– بعد تحليل ومقارنة النتائج التي تم الحصول عليها يتم تتوثيق الدراسة.

(Appendix 2)

يوضح هذا الملحق أحد عمليات التحليل لي بيانات التي تم تجميعها في وقت خارج الذروة، وتم في هذا الوقت استهلاك كمية كبيرة من البيانات يفوق استهلاك اوقات الذروة، وعليه تم القيام بعمليات التحليل لمعرفة سبب هذا الأرتفاع، والذي كان بسبب أستخدام مواقع (Social Media) تستهلك كمية كبيرة من البيانات، التى غالبا تكون عبارة عن فيديوهات ذات جودة عالية.



الشكل(2.7) يوضح أستخدام تطبيق (Snapchat)



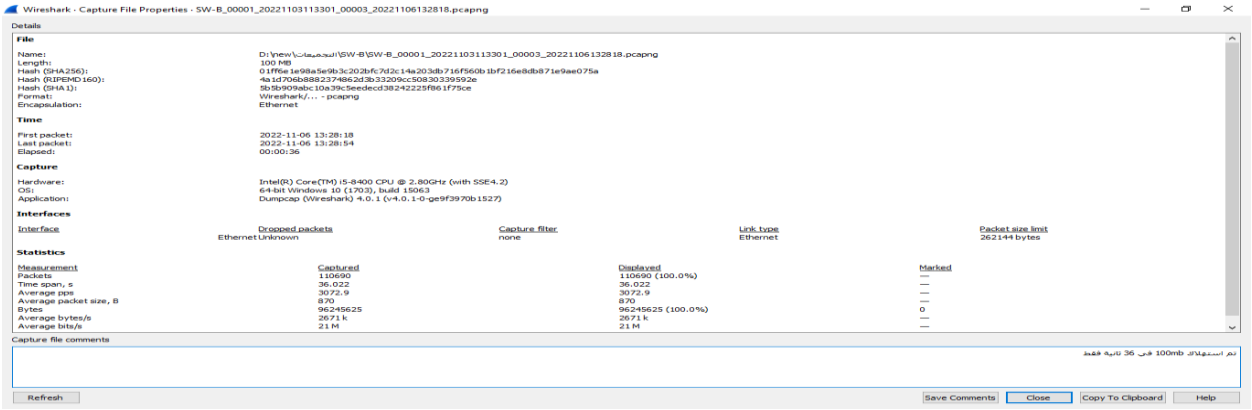
الشكل(3.7) يوضح أستخدام تطبيق (instagram)

(Appendix 3)

في هذا الملحق تم إدراج تقرير عام من برنامج (Wireshark)، يوضح بشكل عام أحد عينات التي تم تجميعها، ومعرفة ايضاً كمية الأستهلاك، ومتوسط الحسابي له، وتوقيت اول واخر (Packet) دخلت للشبكة، ومتوسط الأستهلاك في الثانية الواحدة، والوقت الأجمالية الذي أخذتها عملية المراقبة، وسيتم توضيح خصائص كمية استهلاك البيانات بتاريخ 6-11-2022 في وقت من أوقات ذروة الشبكة.

الشكل(4.7) يوضح خصائص عامة لعملية مراقبة من (Switch-B)

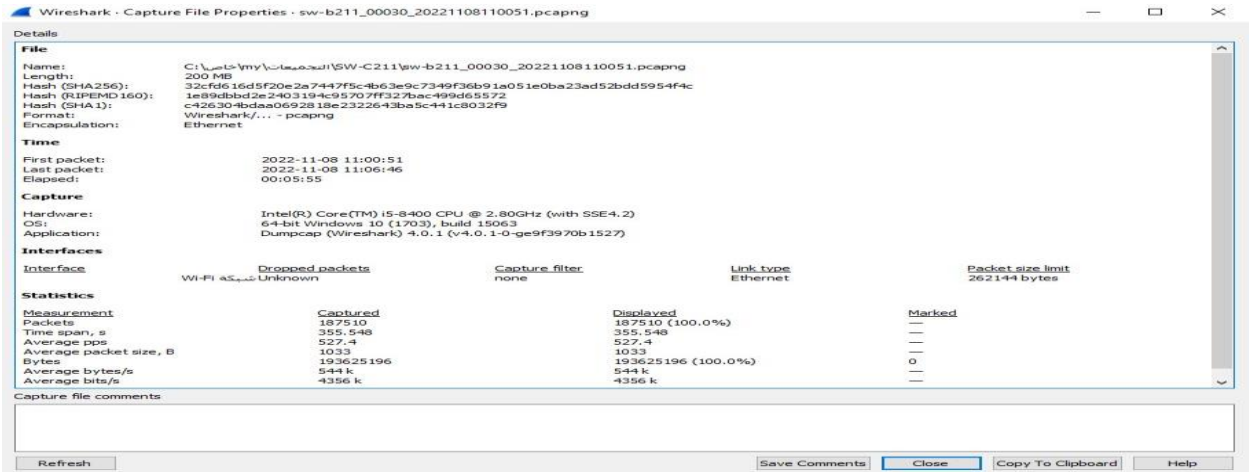
تم استهلاك 100MB في خلال 50 ثانية بمعدل 15MB في الثانية الواحدة.



الشكل(5.7) يوضح خصائص عامة لعملية مراقبة من (Switch-B)

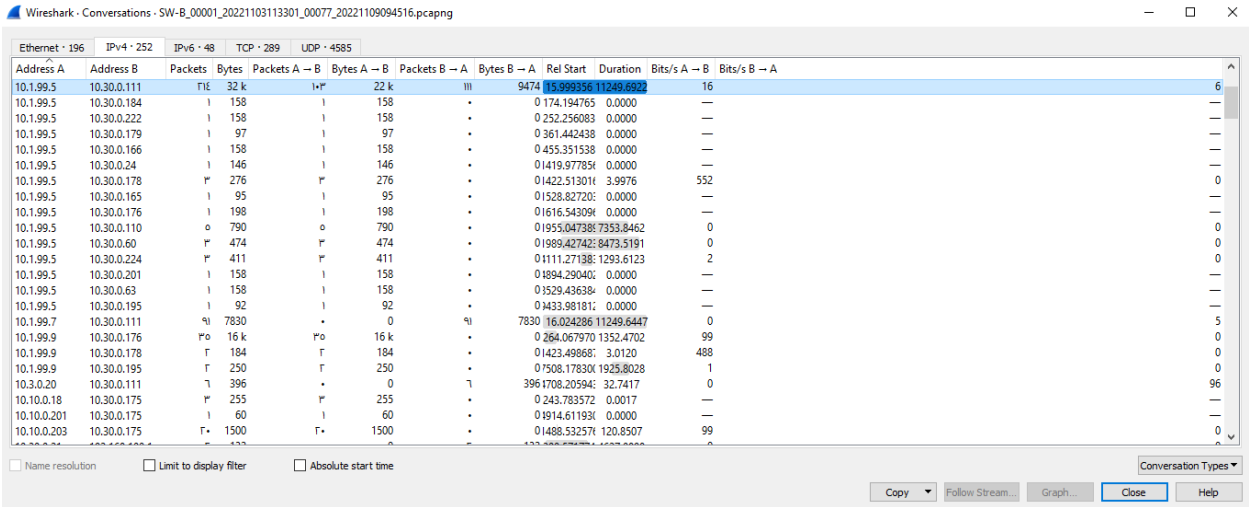
تم استهلاك 100MB في خلال 36 ثانية بمعدل 21MB في الثانية الواحدة.

Appendix 4



الشكل(5.7) يوضح خصائص عامة لعملية مراقبة من (Switch-C) قسم الشبكات

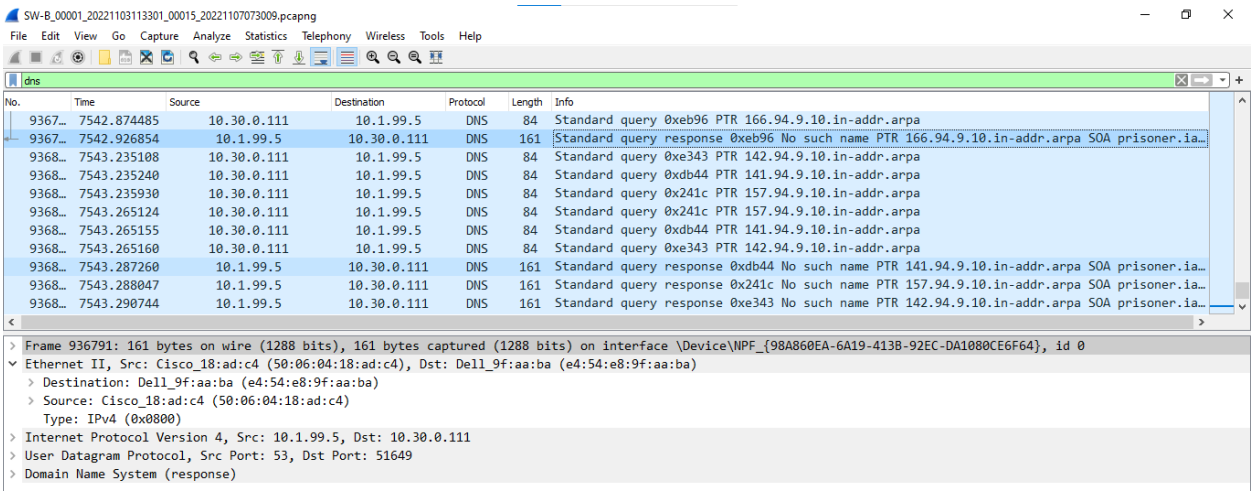
تم استهلاك 200MB في خلال 5:55 دقيقة بمعدل 4MB في الثانية الواحدة.



الشكل(6.7) يوضح عمليات الاتصال التي تحدث بين اجهزة (Switch-B) وخوادم شبكة جامعة سبها

توفر خاصية (Conversations) معرفة كافة المحادثات التى تمت في الشبكة بين الاجهزة والمستخدمين، بشكل مفصل بشكل تسلسلى، وكذلك عدد (Packets) وحجم (Bytes) في كل عملية اتصال بشكل مفصل.

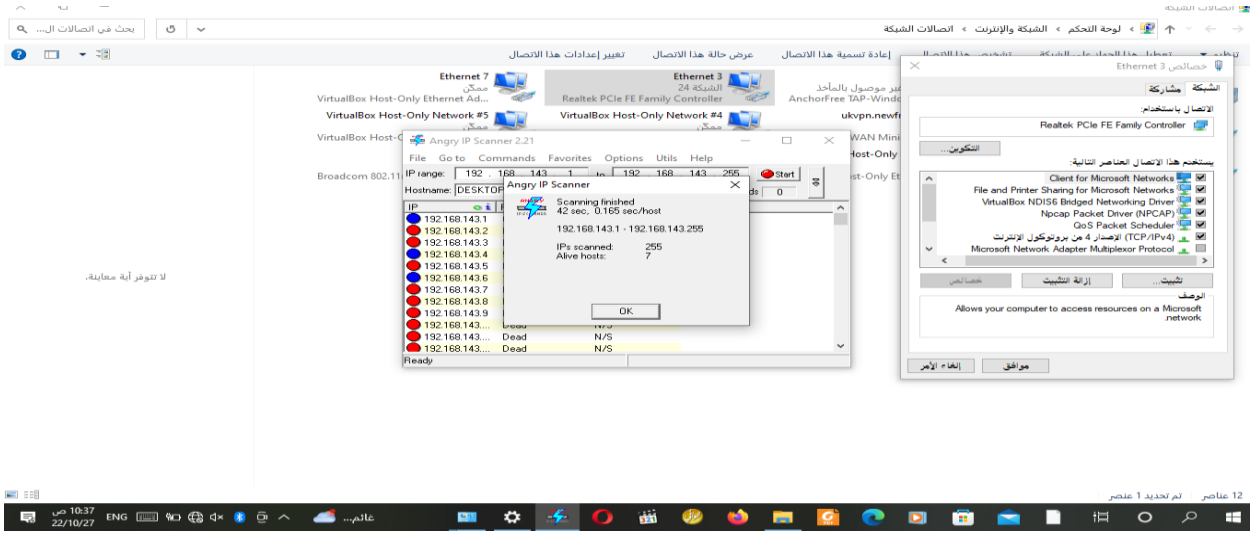
Appendix 5



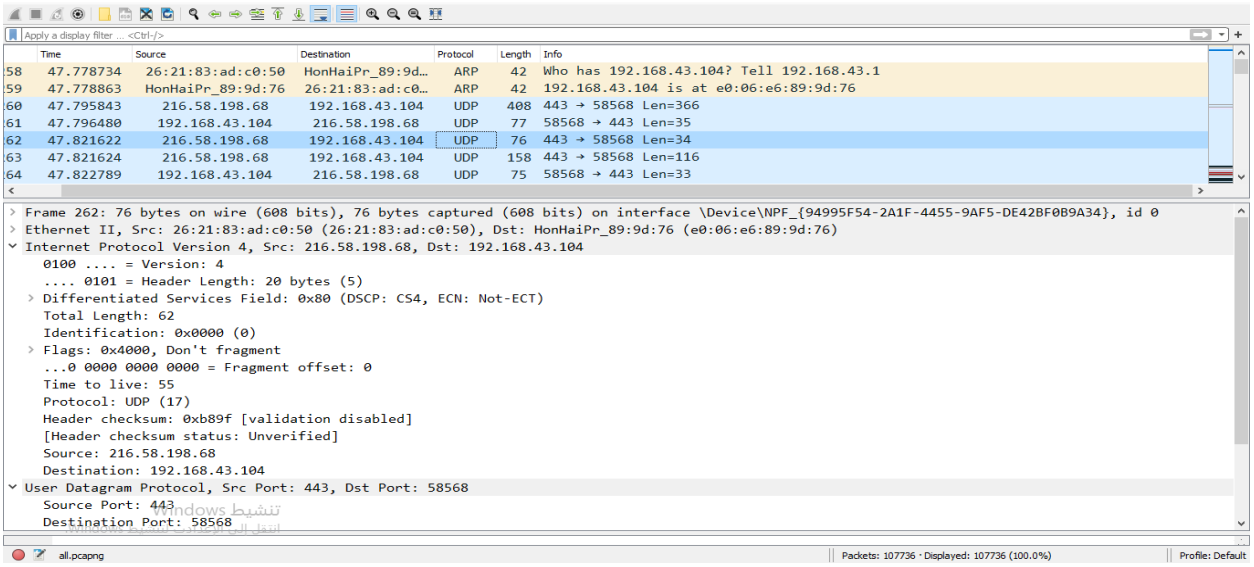
الشكل(7.7) يوضح اتصال بين مستخدم وخادم (Cisco)

في الشكل السابق تظهر عملية تفاعل بين مستخدم في شبكة كلية العلوم يملك (IP) تحت عنوان (10.30.0.11)، و أحد خوادم (Cisco) المتواجد في مركز تقنية المعلومات يملك (IP) تحت عنوان(10.1.99.5)، في عملية التحليل يجب أن يتم معرفة عناوين (IP) التى تكون من خارج الشبكة وحدث تبادل بيانات مع المستخدمين المحليين، ومعرفة سبب هذا الأتصال، وهوية (IP) الخارجي لتأكد من إذ ما كان مستخدم عادي أو مخترق، والتأكد ان هذا الاتصال ليس عملية قرصنة أو تنصت قد تسبب المشاكل لشبكة، بسبب سرقة البيانات أو زرع برمجايات خبيثة داخل الشبكة ليستمر هذا المخترق في عملية القرصنة وسرقة أكبر قدر من البيانات لي أطول فترة ممكنة.

Appendix 6



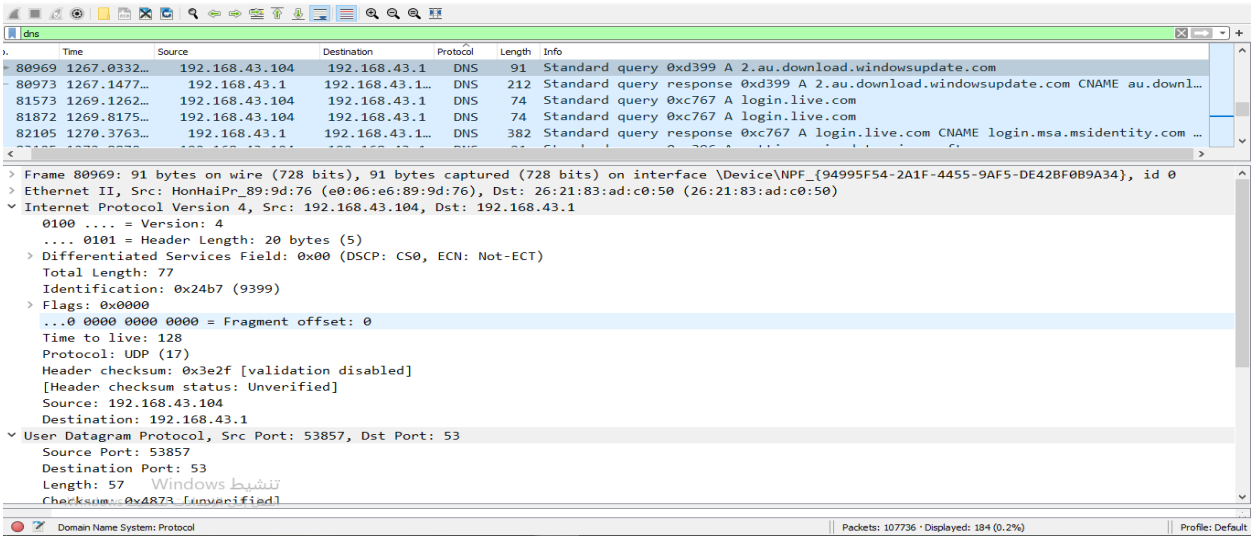
الشكل(8.7) يوضح استخدام برنامج (IPScaner) لمعرفة عدد المستخدمين في شبكة الخاصة بي (Switch-C)



الشكل(9.7) يوضح عملية دخول أحد الاجهزة لشبكة (Switch-C)

Appendix 7

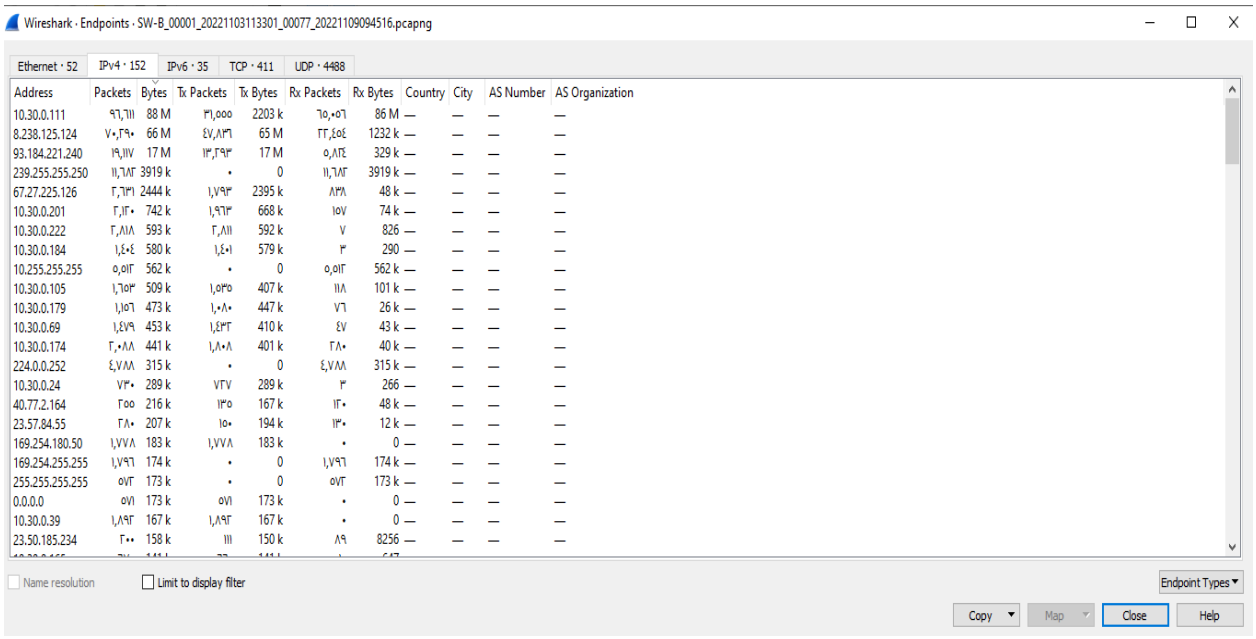
الشكل(8.7)، يوضح أن هناك جهاز يحمل (IP) 192.168.43.104 يحاول الدخول علي الشبكة الخاصة بشبكة قسم الشبكات، وبعد نجاحه في تسجل الدخول عن طريق كتابة (Password) بشكل صحيح، ومن ثم تم إعطائه (Mac Addres) خاص به تحت عنوان (e0:06:e6:89:9d:76).



الشكل(10.7) يوضح قيام مستخدم من شبكة (SW-C) بتنزيل تحديثات لنظام تشغيل (Windows)

عند مراقبة شبكة (SW-C)، تمت ملاحظة ظهور ارتفاع في وقت خارج وقت الذروة، في الساعة 8:27 صباحاً، حيث تمت في تلك الفترة استهلاك قرابة (3GB) في اقل من 30 دقيقة، وعند تحليل البيانات في تلك الفترة، وجدنا أن الموظف الذي يمتلك عنوان (IP) بعنوان 192.168.43.104 قام بأستهلاك ما يقرب من (1.9GB)، وذلك بسبب قيامه بتنزيل تحديثات لنظام تشغل (Windows).

Appendix 8



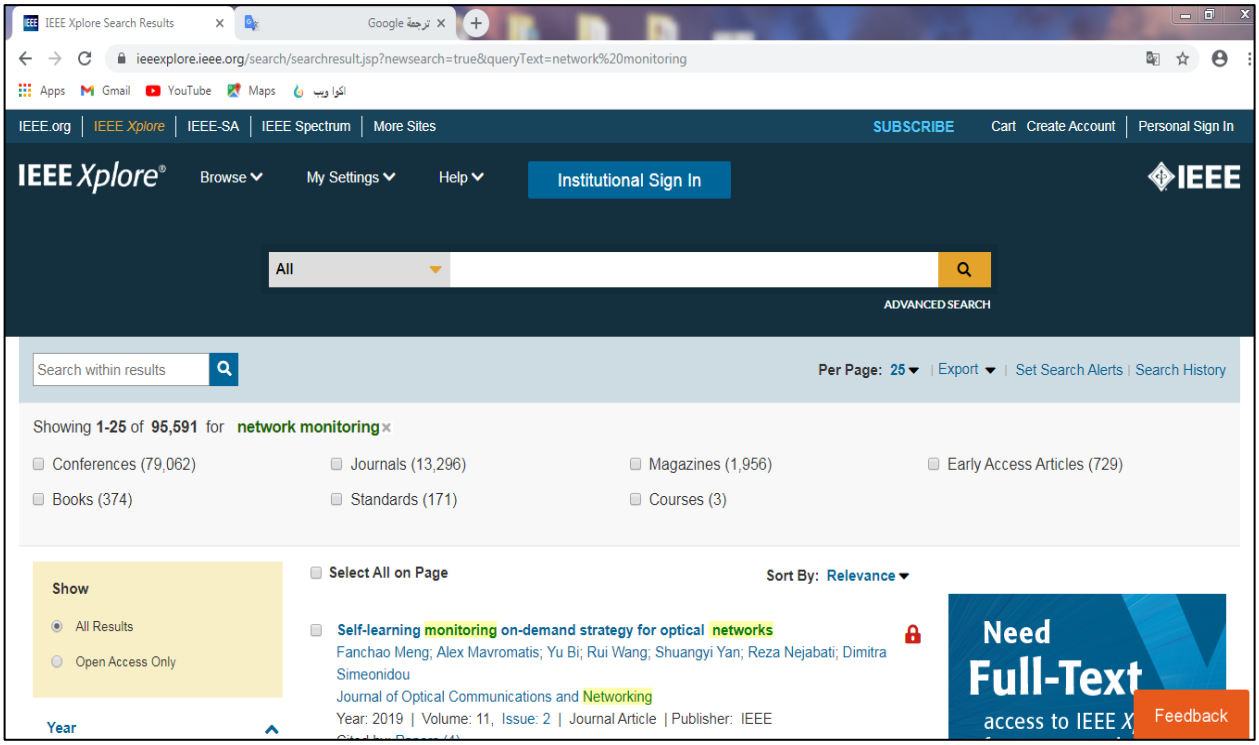
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
10.30.0.111	٩٦,٦١١	88 M	٣١,٥٥٥	2203 k	٦٥,٠٥٦	86 M	—	—	—	—
8.238.125.124	٧٠,٢٩٠	66 M	٤٧,٨٣٦	65 M	٢٢,٤٥٤	1232 k	—	—	—	—
93.184.221.240	١٩,١١٧	17 M	١٣,٢٩٣	17 M	٥,٨٢٤	329 k	—	—	—	—
239.255.255.250	١١,٦٨٢	3919 k	٠	0	١١,٦٨٢	3919 k	—	—	—	—
67.27.225.126	٢,٦٣١	2444 k	١,٧٩٣	2395 k	٨٣٨	48 k	—	—	—	—
10.30.0.201	٢,١٢٠	742 k	١,٩٦٣	668 k	١٥٧	74 k	—	—	—	—
10.30.0.222	٢,٨١٨	593 k	٢,٨١١	592 k	٧	826	—	—	—	—
10.30.0.184	١,٤٠٤	580 k	١,٤٠١	579 k	٣	290	—	—	—	—
10.255.255.255	٥,٥١٢	562 k	٠	0	٥,٥١٢	562 k	—	—	—	—
10.30.0.105	١,٦٥٣	509 k	١,٥٣٥	407 k	١١٨	101 k	—	—	—	—
10.30.0.179	١,١٥٦	473 k	١,٠٨٠	447 k	٧٦	26 k	—	—	—	—
10.30.0.69	١,٤٧٩	453 k	١,٤٣٢	410 k	٤٧	43 k	—	—	—	—
10.30.0.174	٢,٠٨٨	441 k	١,٨٠٨	401 k	٢٨٠	40 k	—	—	—	—
224.0.0.252	٤,٧٨٨	315 k	٠	0	٤,٧٨٨	315 k	—	—	—	—
10.30.0.24	٧٣٠	289 k	٧٢٧	289 k	٣	266	—	—	—	—
40.77.2.164	٢٥٥	216 k	١٣٥	167 k	١٢٠	48 k	—	—	—	—
23.57.84.55	٢٨٠	207 k	١٥٠	194 k	١٣٠	12 k	—	—	—	—
169.254.180.50	١,٧٧٨	183 k	١,٧٧٨	183 k	٠	0	—	—	—	—
169.254.255.255	١,٧٩٦	174 k	٠	0	١,٧٩٦	174 k	—	—	—	—
255.255.255.255	٥٧٢	173 k	٠	0	٥٧٢	173 k	—	—	—	—
0.0.0.0	٥٧١	173 k	٥٧١	173 k	٠	0	—	—	—	—
10.30.0.39	١,٨٩٢	167 k	١,٨٩٢	167 k	٠	0	—	—	—	—
23.50.185.234	٢٠٠	158 k	١١١	150 k	٨٩	8256	—	—	—	—

الشكل(9.7) يوضح كمية استهلاك كل مستخدم في شبكة (SW–B)

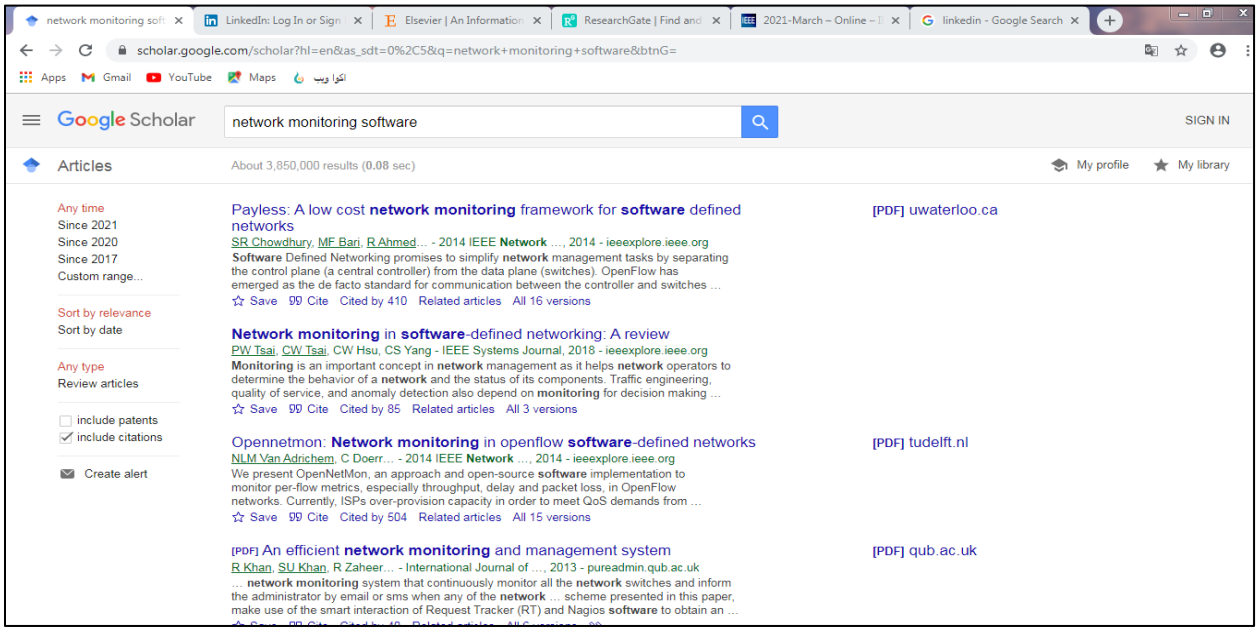
بواسطة خاصية (Endpoint)، يمكن لمحلل الشبكة معرفة كافة مستخدمي الشبكة، وكذلك يمكن له أن يعلم بكمية إستهلاك كل جهاز، ونوع البروتوكولات التي يقوم بإستخدامها طوال فترة تواجده في الشبكة.

Appendix 9

IEEE: Network monitoring

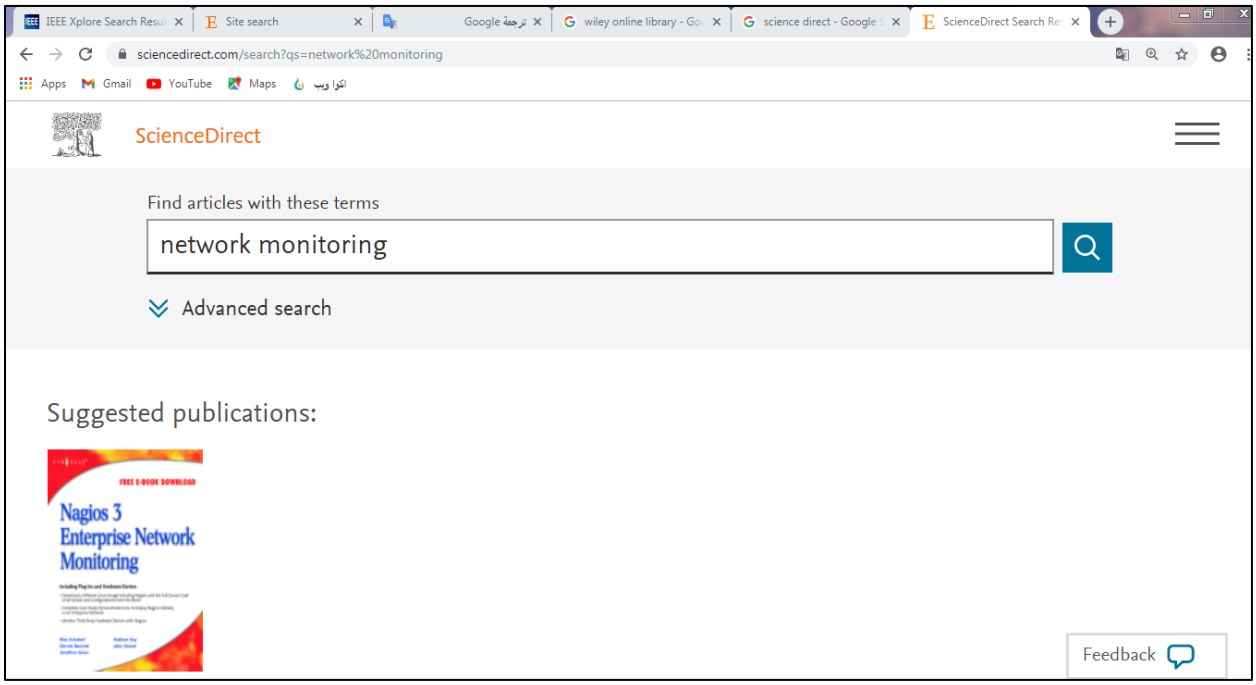


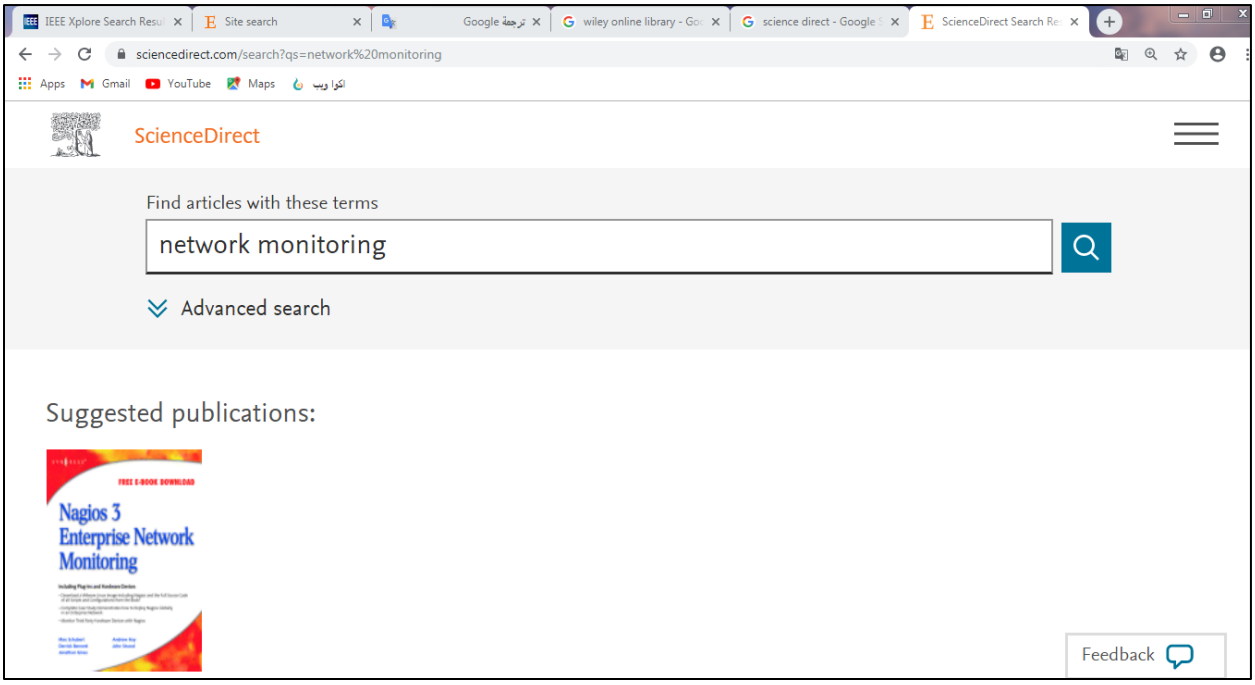
Google Scholar: Network monitoring software



Appendix 10

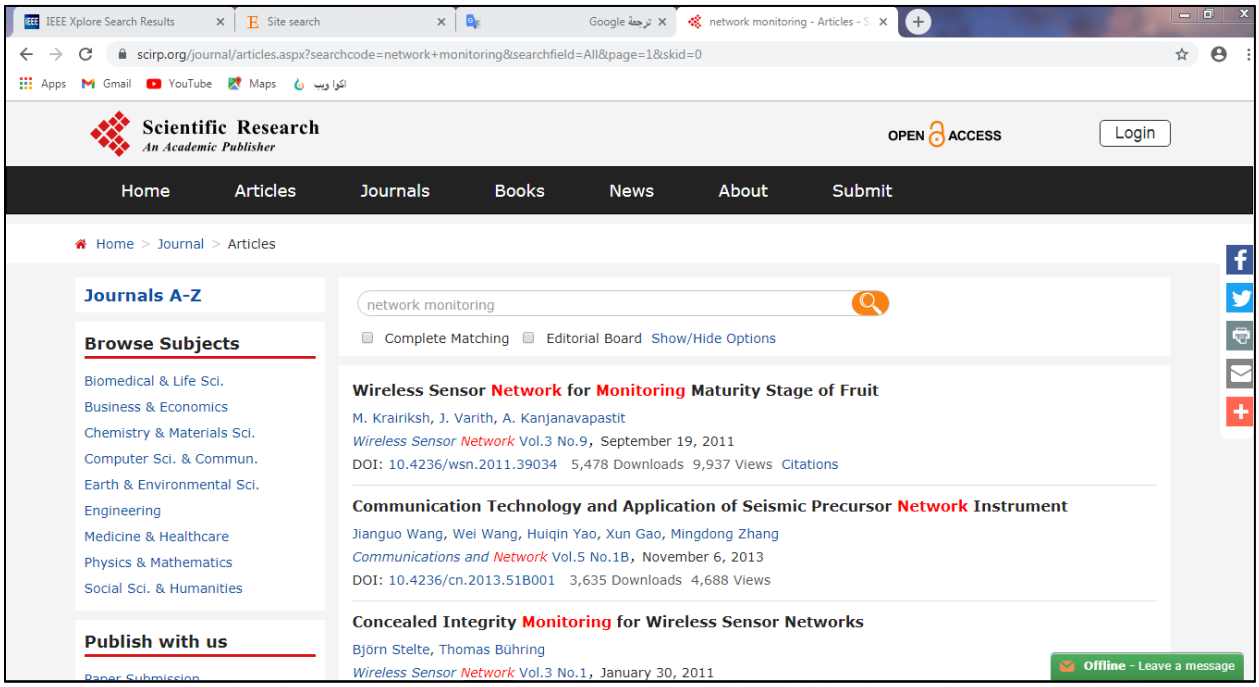
Sciencedirect: Network Monitoring

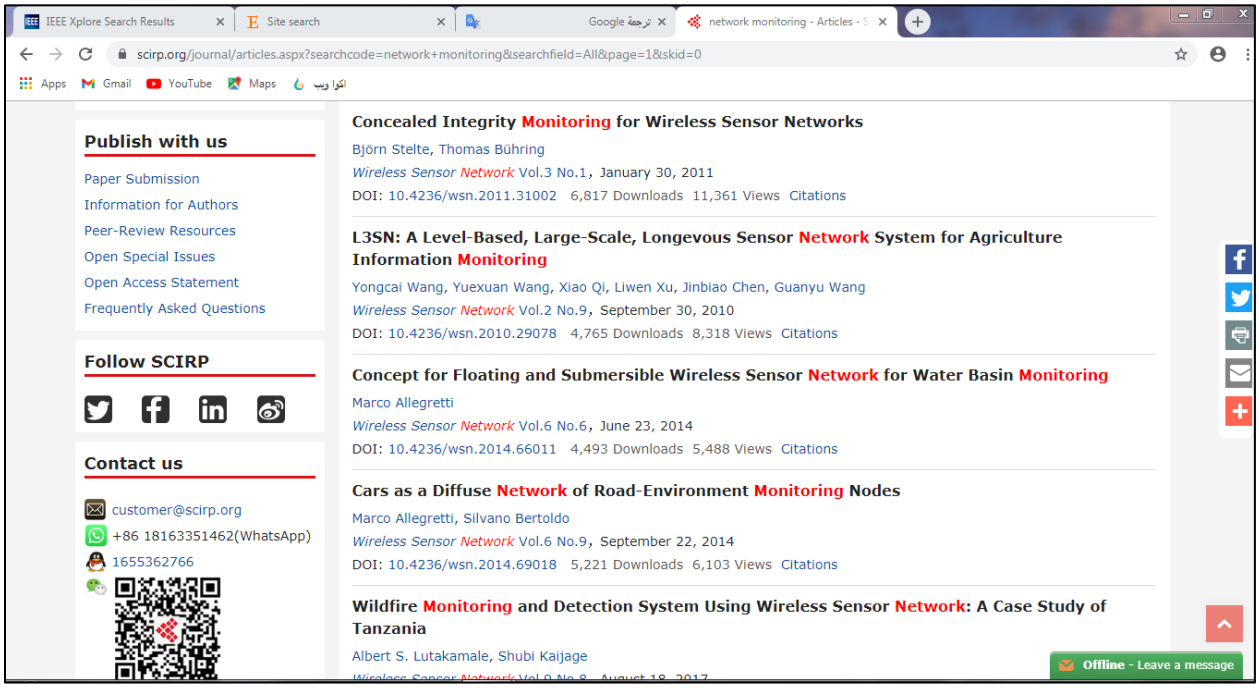




Appendix 11

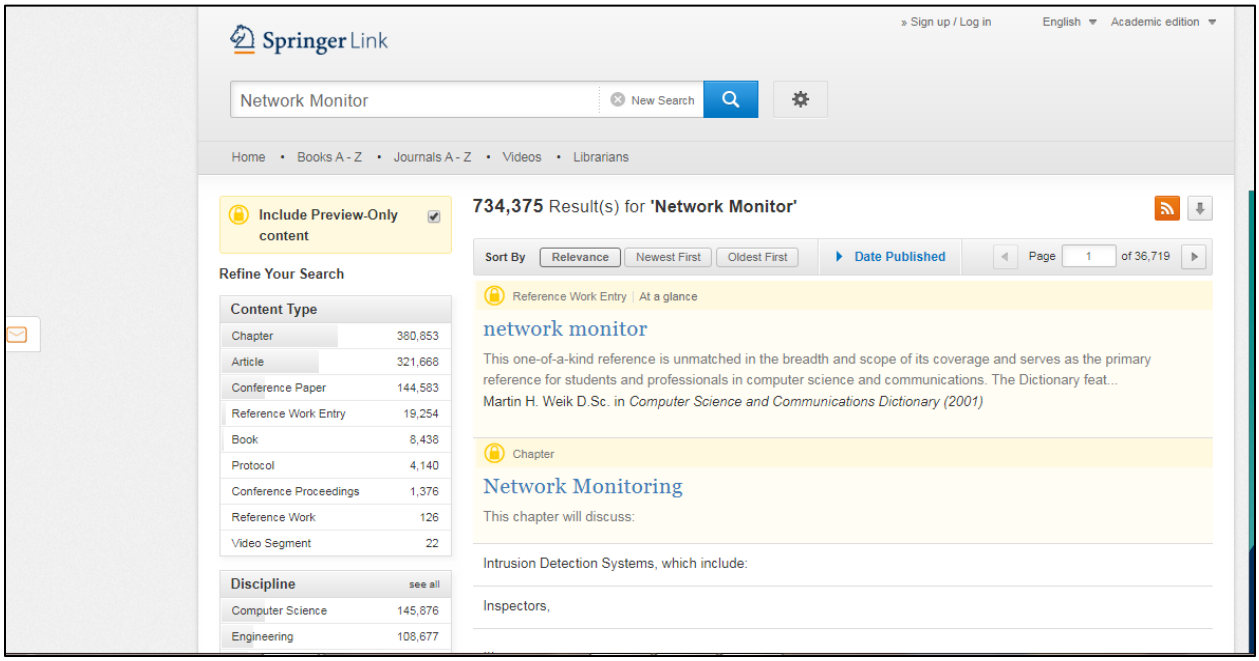
Scientific Research: Network Monitoring Problem.





Appendix 12

Springer Link: Network Monitor



Appendix 13

Gantt Chart

Tasks		2022					2023				
		A	S	O	N	D	J	F	M	A	M
قراءة الدراسات السابقة	Literature Review	■	■	■							
دراسة المتغيرات ووضع المنهجية	Research Problem			■							
	Research Questions			■							
	Research Objectives			■							
	Methodology			■							
مرحلة التصميم	Research Design			■							
مرحلة التنفيذ	Implementation			■	■	■					
التقييم وكتابة التقرير	Evaluation and Reporting					■	■				
قراءة الدراسات السابقة	Literature Review	##	##	##							
دراسة المتغيرات ووضع المنهجية	Research Problem			##							
	Research Questions			##							
	Research Objectives			##							
	Methodology			##							
مرحلة التصميم	Research Design			##							
مرحلة التنفيذ	Implementation			##	##	##					
التقييم وكتابة التقرير	Evaluation and Reporting					##	##				