دليل شامل لأداة Wireshark
الجزء الثاني

مرحباً بك في الدليل المتقدم لأداة Wireshark، حيث ستتعلم تقنيات التحليل المتقدمة، الأوامر الكاملة، والأسرار التي تجعلك خبيراً في تحليل حركة الشبكة.

أوامر كاملة

فلاتر متقدمة، أوامر خطية، واختصارات لتحليل فعال

تحليل أمني

كشف الهجمات، تحليل التهديدات، وحماية الشبكات

رسوم بيانية

تصورات متقدمة، تحليلات مرئية، وتقارير تفصيلية

مهام عملية

تمارين واقعية، سيناريوهات تطبيقية، وحالات دراسية

تحليل متقدم

بروتوكولات معقدة، حركة مشفرة، واستكشاف أخطاء

أسرار احترافية

نصائح الخبراء، تقنيات متقدمة، وأفضل الممارسات

من إعداد: **أ. عبد الصمد بوركيبات**
باحث في فقه الأمن السيبراني الأسري، ومتخصص في الأمن السيبراني

مرجع أوامر Wireshark الشامل

فلاتر الالتقاط، فلاتر العرض، العوامل المنطقية، واختصارات لوحة المفاتيح

فلاتر الالتقاط

النوع	مثال
عنوان IP	`host 192.168.1.1`
منفذ TCP/UDP	`tcp port 80`
نطاق IP	`net 192.168.1.0/24`
بروتوكول	`tcp or udp`
عنوان MAC	`ether host 00:0c:29:12:34:56`

فلاتر العرض

النوع	مثال
عنوان IP	`ip.addr == 192.168.1.1`
عنوان المصدر	`ip.src == 192.168.1.1`
عنوان الوجهة	`ip.dst == 192.168.1.1`
المنفذ	`tcp.port == 80`
البروتوكول	`tcp or http`

العوامل المنطقية والمقارنة

العامل	الوصف	مثال
`and`	منطقي AND	`ip.addr == 192.168.1.1 and tcp.port == 80`
`or`	منطقي OR	`tcp.port == 80 or tcp.port == 443`
`==`	يساوي	`ip.addr == 192.168.1.1`
`=!`	لا يساوي	`ip.addr != 192.168.1.1`

اختصارات لوحة المفاتيح

- Ctrl+E - بدء/إيقاف الالتقاط
- Ctrl+F - البحث في الحزم
- Ctrl+↓ - الحزمة التالية
- Ctrl+↑ - الحزمة السابقة
- Ctrl+Shift+C - تلوين الحزم
- Ctrl+S - حفظ الالتقاط
- Ctrl+O - فتح ملف
- Ctrl+N - الانتقال إلى الحزمة

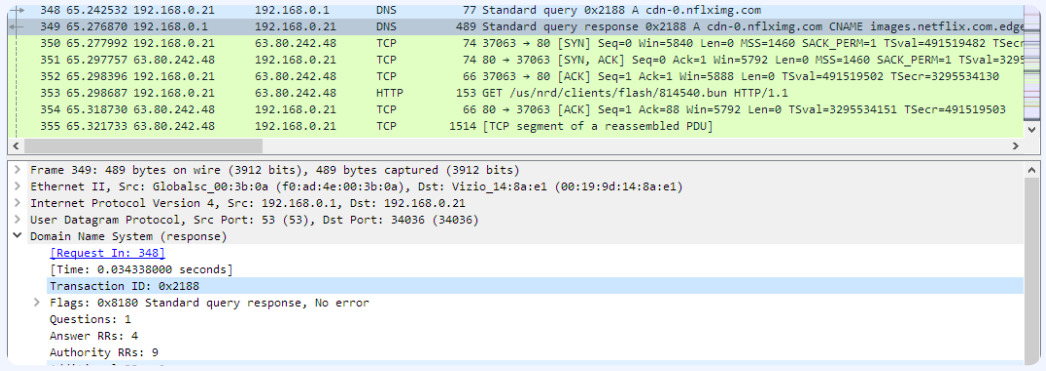
نصيحة:
استخدم `!` للنفي في فلاتر العرض، مثال: `tcp!` لعرض جميع الحزم غير TCP

تقنيات التحليل المتقدمة

متابعة تدفقات البروتوكول، تحليل TCP، إعادة تجميع الحزم، وتحليل المعلومات الخبيرة

متابعة تدفقات البروتوكول

- **TCP Stream:** تحليل اتصالات TCP الكاملة
- **HTTP Stream:** عرض طلبات وردود HTTP
- **SSL/TLS:** فك تشفير الجلسات المشفرة
- **UDP Stream:** تحليل تدفقات UDP

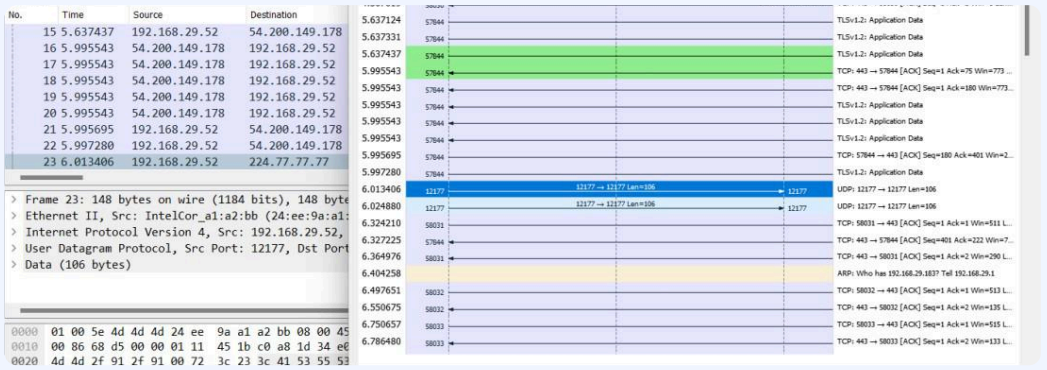


نصيحة

استخدم **Analyze → Follow → TCP Stream** لعرض محادثة TCP كاملة

تحليل TCP وإعادة التجميع

- **TCP Flags:** تحليل SYN، ACK، FIN، RST
- **Sequence/Ack:** تتبع أرقام التسلسل والتأكيد
- **Retransmission:** كشف إعادة الإرسال
- **Window Size:** تحليل حجم النافذة

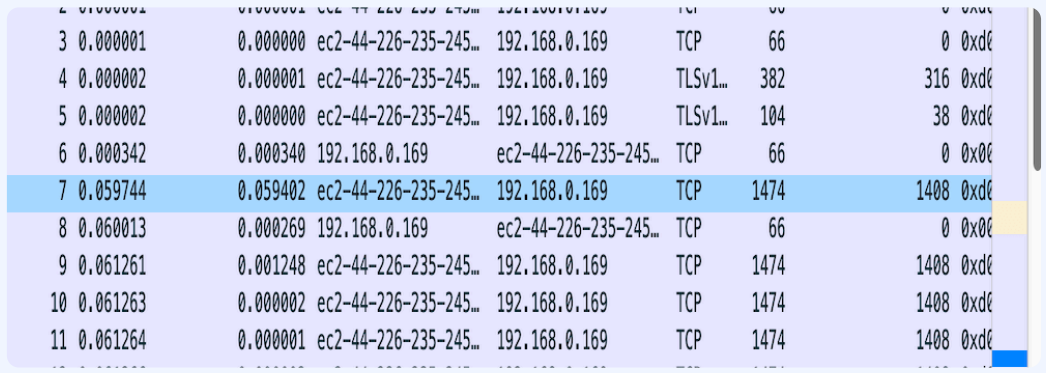


نصيحة

تفعيل **TCP Analysis** من **Analyze → Expert Info** لكشف المشاكل

تقنيات إعادة تجميع الحزم

- **IP Defragmentation:** إعادة تجميع أجزاء IP
- **TCP Reassembly:** إعادة تجميع شرائح TCP
- **SMB Reassembly:** إعادة تجميع ملفات SMB
- **HTTP Objects:** استخراج كائنات HTTP

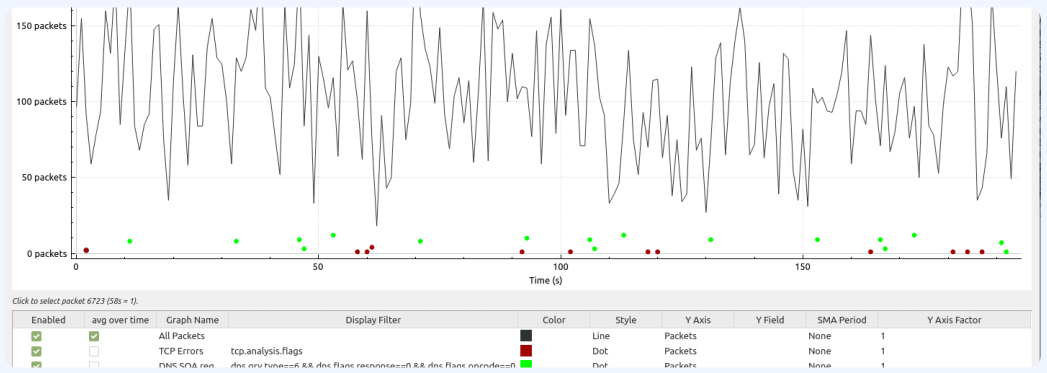


نصيحة

استخدم **HTTP → Export Objects → File...** لاستخراج الملفات

تحليل المعلومات الخبيرة

- **Expert Info:** عرض المشاكل والتحذيرات
- **Colorization:** تلوين الحزم حسب الأهمية
- **Notes:** إضافة ملاحظات للحزم
- **Comments:** إضافة تعليقات للتحليل



نصيحة

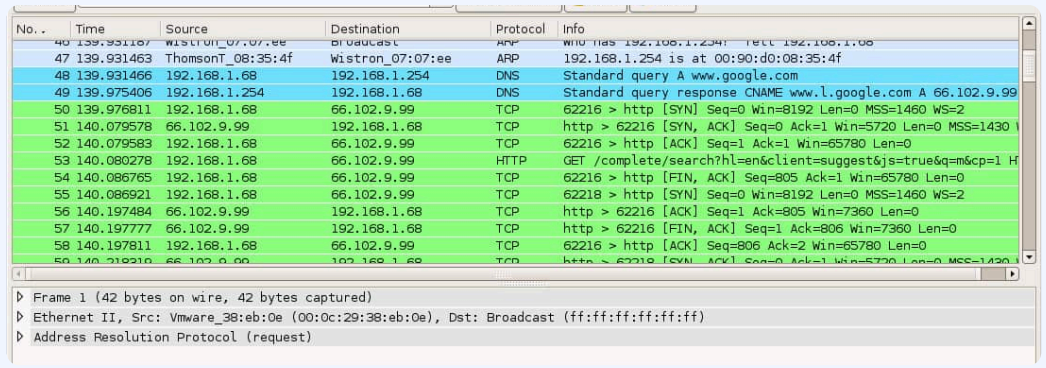
تفعيل **View → Coloring Rules** لتخصيص ألوان الحزم

تحليل الأمان مع Wireshark

كشف عمليات المسح، هجمات ARP، تحليل البرامج الضارة، وفك تشفير جلسات SSL/TLS

كشف عمليات مسح Nmap

- **TCP Connect:** إكمال المصافحة الثلاثية
- **SYN Scan:** إرسال حزم SYN دون إكمال المصافحة
- **UDP Scan:** فحص المنافذ المغلقة عبر رسائل ICMP
- **خصائص:** حجم النافذة، أنماط الحزم، التوقيت

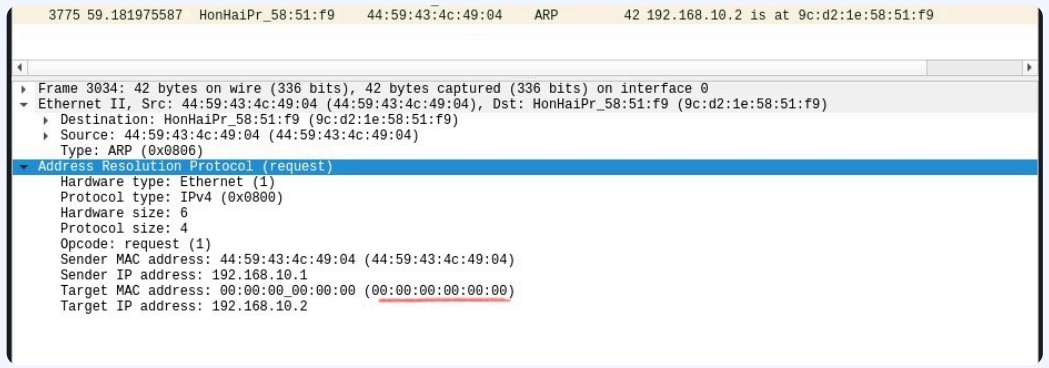


فلتر كشف TCP Connect

```
tcp.flags.syn == 1 and tcp.flags.ack == 0
```

كشف هجمات ARP و MITM

- **ARP Poisoning:** تزوير عناوين MAC
- **Duplicate ARP:** استجابات ARP مكررة
- **gratuitous ARP:** حزم ARP غير مطلوبة
- **MITM:** اعتراض وتحويل حركة المرور

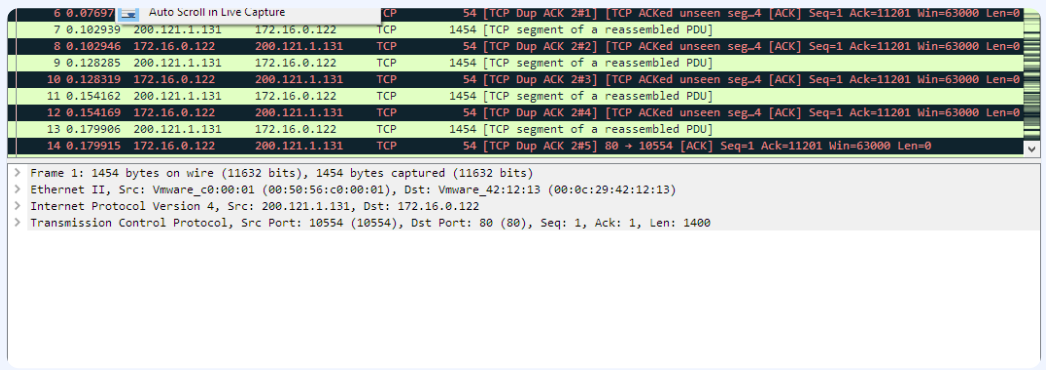


فلتر كشف ARP غير طبيعي

```
arp.duplicate-address-detected
```

تحليل سلوك البرامج الضارة

- **Beaconing:** اتصالات منتظمة بخوادم التحكم
- **DNS Tunneling:** استخدام DNS لتمرير البيانات
- **Anomalous Traffic:** حركة مرور غير معتادة
- **Exfiltration:** تسريب البيانات

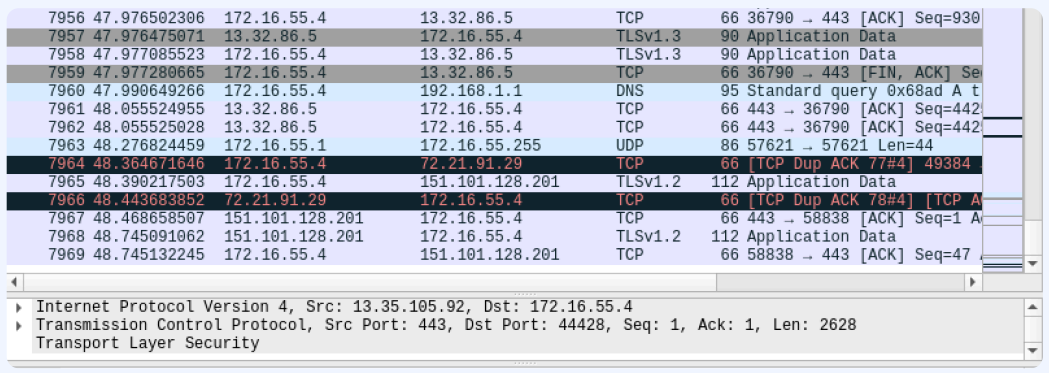


فلتر كشف الاتصالات المنتظمة

```
frame.time_delta > 10 && frame.time_delta < 60
```

فك تشفير جلسات SSL/TLS

- **Server Key:** استخدام مفتاح الخادم الخاص
- **SSLKEYLOGFILE:** متغير البيئة للمتصفحات
- **Pre-Master Secret:** تسجيل مفاتيح الجلسة
- **Decrypted Traffic:** عرض البيانات المشفرة



إعداد Wireshark لفك التشفير

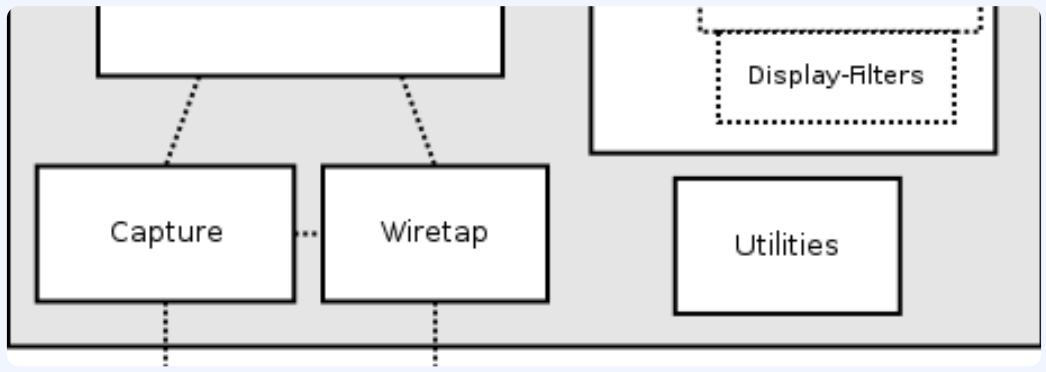
```
Edit → Preferences → Protocols → SSL → (Pre)-Master-Secret log filename
```

التحليل البصري والرسوم البيانية

رسوم الحزم، رسوم I/O، خرائط GeoIP، وتصور هرميات البروتوكول

رسوم الحزم (Packet Diagrams)

- **عرض مرئي:** تمثيل بصري للحزم والحقول
- **تفاعلي:** النقر على العناصر لتمييزها
- **عرض القيم:** إظهار قيم الحقول
- **فلاتر:** عرض فلتر عند التمرير

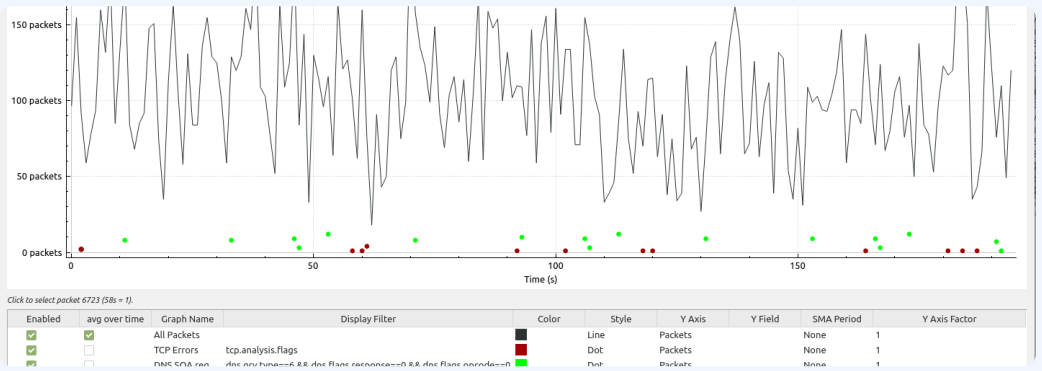


تفعيل الميزة

Edit → Preferences → Layout → Packet Diagram

رسوم I/O لتحليل حركة المرور

- **رسوم بيانية:** تمثيل حركة المرور عبر الزمن
- **فلاتر متقدمة:** تطبيق فلاتر على الرسوم
- **مقارنة:** مقارنة بروتوكولات متعددة
- **تصدير:** حفظ الرسوم للتحليل

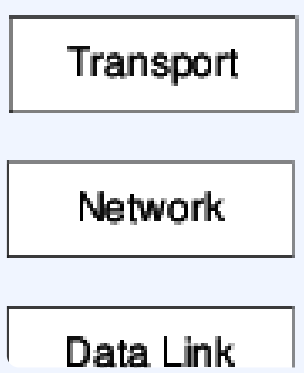


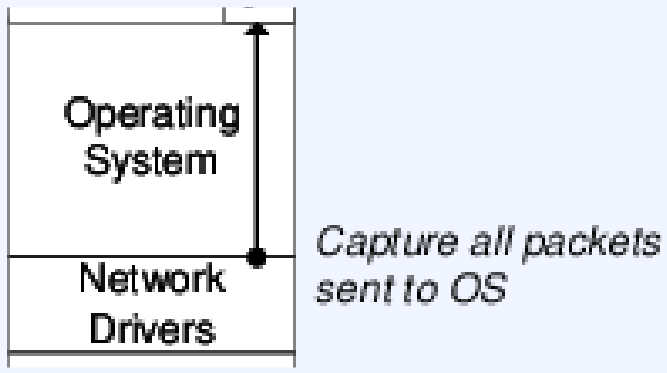
الوصول للميزة

Statistics → I/O Graph

خرائط GeoIP

- **تحديد الموقع:** تحديد المواقع الجغرافية
- **فلترة:** فلترة حسب الدولة/المنطقة
- **ASN:** تحديد أرقام أنظمة المستقل
- **قواعد البيانات:** استخدام Maxmind GeoLite



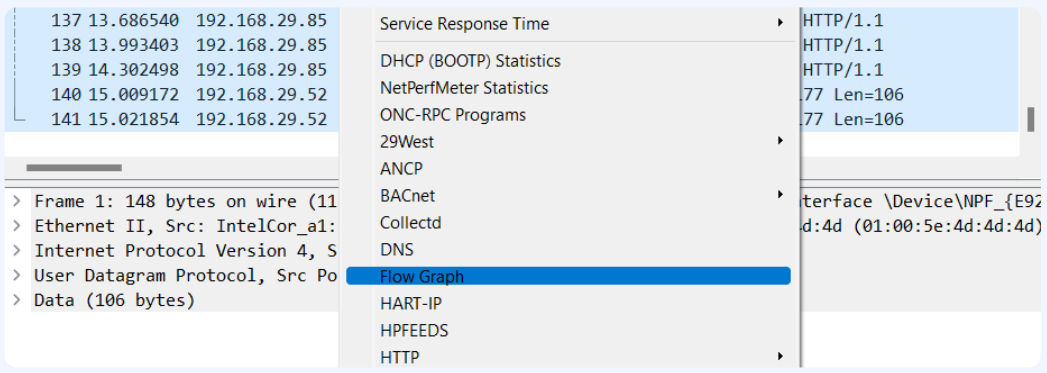


فلترة حسب الموقع

ip and not ip.geoip.asnum == 63949

تصور هرميات البروتوكول

- **هرم OSI:** عرض طبقات الشبكة
- **تسلسل:** عرض تسلسل البروتوكولات
- **تحليل:** تحليل العلاقات بين البروتوكولات
- **إحصائيات:** إحصائيات البروتوكولات



عرض إحصائيات البروتوكول

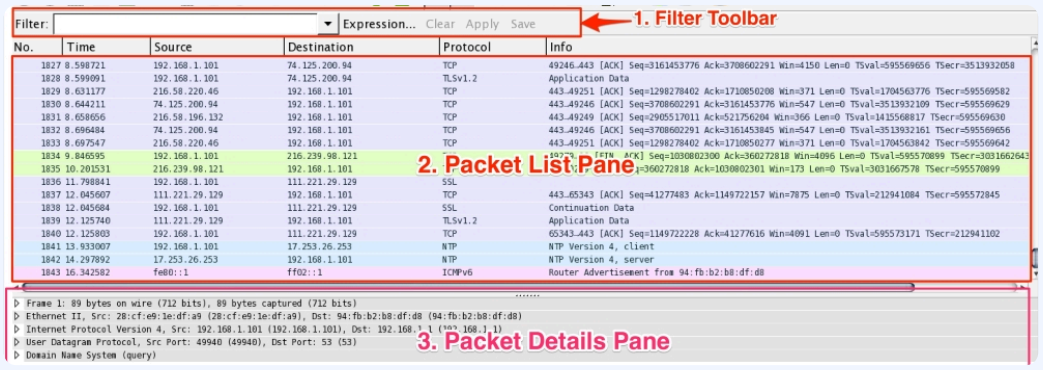
Statistics → Protocol Hierarchy

المهام والتمارين العملية

تمارين تحليل خطوة بخطوة، سيناريوهات واقعية، استكشاف أخطاء الشبكة، ودراسات حالة للتحقيقات الأمنية

تمارين تحليل خطوة بخطوة

1. **التقاط الحزم:** تحديد واجهة الشبكة وتطبيق الفلاتر
2. **تحليل البروتوكول:** فحص حزم TCP/UDP/HTTP
3. **متابعة التدفقات:** استخدام Follow TCP Stream
4. **استخراج البيانات:** تصدير الكائنات من الحزم

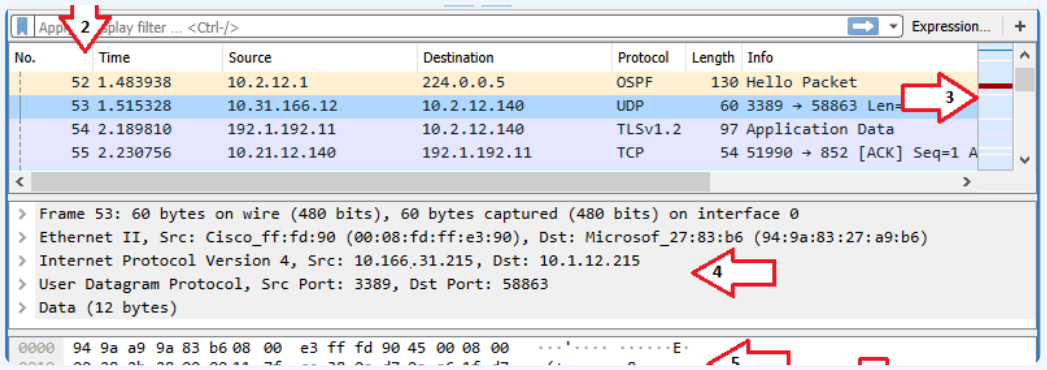


مهمة عملية

التقط حركة مرور HTTP وقم بتحليل الطلبات والردود باستخدام Follow TCP Stream

سيناريوهات واقعية

- **بطء الشبكة:** تحديد أسباب التأخير
- **انقطاع الاتصال:** تحليل فقدان الحزم
- **تطبيقات بطيئة:** تشخيص مشاكل التطبيقات
- **ازدحام الشبكة:** تحديد مصادر الازدحام

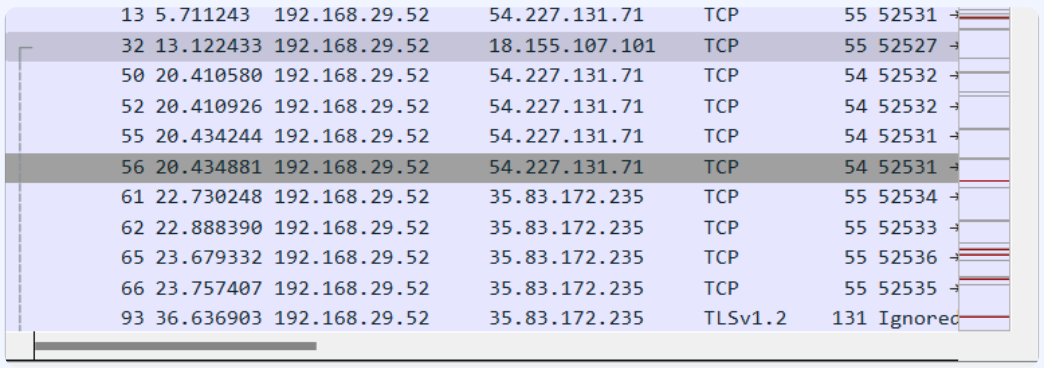


مهمة عملية

حلل ملف PCAP يحتوي على مشكلة بطء في التصفح وحدد السبب

استكشاف أخطاء الشبكة

- **مشاكل DNS:** تحليل استعلامات DNS
- **مشاكل DHCP:** تتبع عملية تخصيص العناوين
- **إعادة الإرسال:** تحليل TCP Retransmission
- **مشاكل ARP:** كشف تضارب عناوين MAC

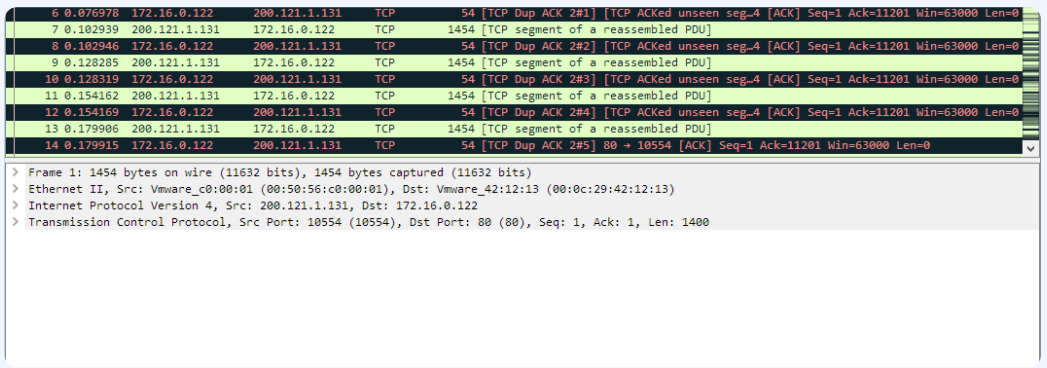


مهمة عملية

استخدم Wireshark لتشخيص مشكلة في اتصال جهاز بالشبكة

دراسات حالة للتحقيقات الأمنية

- **هجوم MITM:** تحليل هجمات الرجل في المنتصف
- **برامج ضارة:** كشف سلوك البرامج الخبيثة
- **مسح الشبكة:** تحديد عمليات المسح غير المصرح بها
- **تسريب البيانات:** تحليل محاولات استخراج البيانات



مهمة عملية

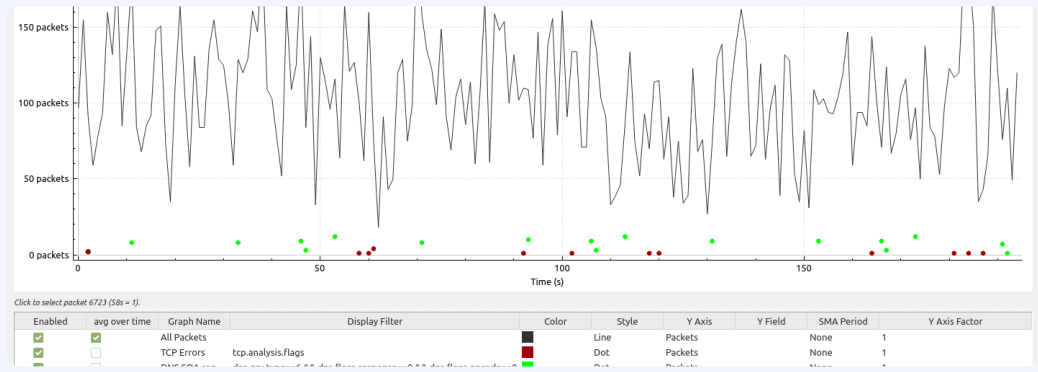
حلل ملف PCAP يحتوي على هجوم ARP Poisoning وحدد الجهاز المهاجم

قضية عملية 1: تحليل أداء الشبكة

تحديد أسباب بطء الشبكة وتحليل زمن الاستجابة وتحديد نقاط الازدحام

خطوات التحليل

- **التقاط البيانات:** بدء التقاط حركة المرور على الواجهة المعنية
- **تطبيق الفلاتر:** استخدام فلاتر لعزل حركة المرور ذات الصلة
- **تحليل I/O Graph:** مراقبة أنماط حركة المرور عبر الزمن
- **فحص الحزم:** تحليل الحزم ذات زمن الاستجابة المرتفع
- **تحديد المشاكل:** البحث عن إعادة الإرسال وفقدان الحزم



الأدوات والفلاتر المستخدمة

فلتر زمن الاستجابة

```
frame.time_delta > 0.1
```

فلتر إعادة الإرسال

```
tcp.analysis.retransmission
```

فلتر فقدان الحزم

```
tcp.analysis.lost_segment
```

أداة إحصائيات نقطة النهاية

```
Statistics → Endpoints → IPv4
```

أداة رسوم I/O

```
Statistics → I/O Graph
```

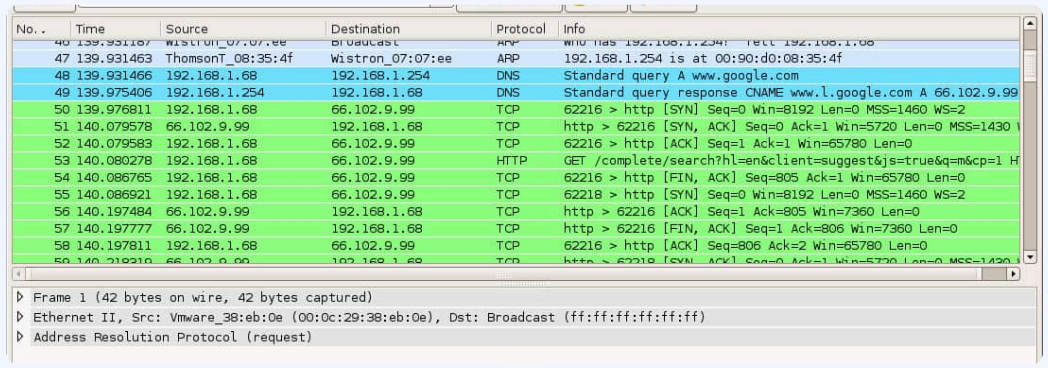
النتائج والتوصيات

- **تحديد نقاط الازدحام:** تحديد الأجهزة أو الروابط المسببة للازدحام
- **تحليل زمن الاستجابة:** حساب متوسط زمن الاستجابة للشبكة
- **تحديد الأسباب:** تحديد ما إذا كان البطء بسبب الأجهزة أو البرمجيات
- **توصيات التحسين:** اقتراح حلول لتحسين أداء الشبكة

مستوى إكمال التحليل: 75%

مهمة عملية

- **تحميل ملف PCAP:** قم بتحميل ملف التقاط شبكة يحتوي على مشكلة أداء
- **تحليل الحزم:** استخدم الفلاتر لتحديد الحزم ذات المشاكل
- **إنشاء رسوم بيانية:** استخدم I/O Graph لتمثيل حركة المرور
- **تقرير النتائج:** قم بإعداد تقرير يلخص النتائج والتوصيات



قضية عملية 2: كشف هجمات الشبكة

استخدام Wireshark للكشف عن هجمات DDoS ومحاولات الاختراق وأنماط الحركة المشبوهة

أنواع الهجمات المشتركة

DDoS | Man-in-the-Middle | Port Scanning

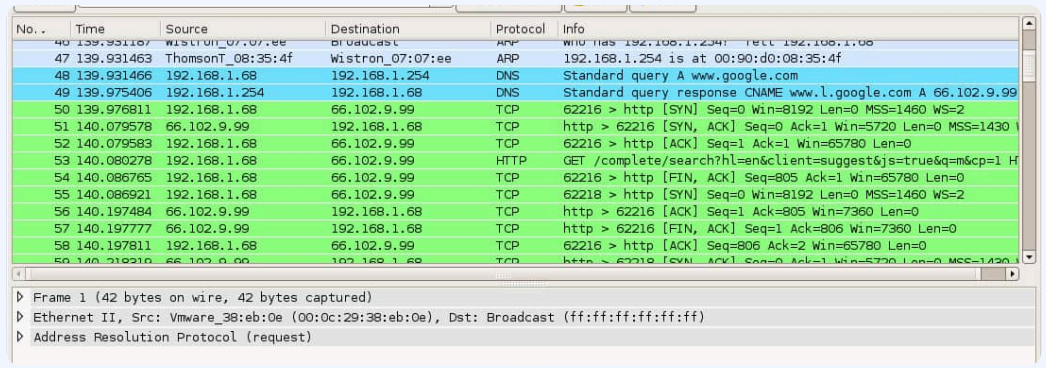
Brute Force | Malware | SQL Injection

هجمات DDoS: فيضان الحزم من مصادر متعددة

MITM: اعتراض وتعديل البيانات أثناء النقل

Port Scanning: فحص المنافذ المفتوحة بحثاً عن ثغرات

Brute Force: محاولات دخول متكررة بكلمات مرور مختلفة



فلاتر الكشف عن الهجمات

كشف هجمات DDoS

```
ip.src==192.168.1.1 && frame.time_delta < 0.01
```

كشف عمليات المسح

```
tcp.flags.syn==1 && tcp.flags.ack==0
```

كشف محاولات الدخول الفاشلة

```
ftp.response.code == 530 ||
ssh.connection.auth_failure
```

كشف هجمات ARP Spoofing

```
arp.duplicate-address-detected
```

كشف أنشطة البرامج الضارة

```
"dns.qry.name matches "(malicious|suspicious)
```

تحليل أنماط الهجمات

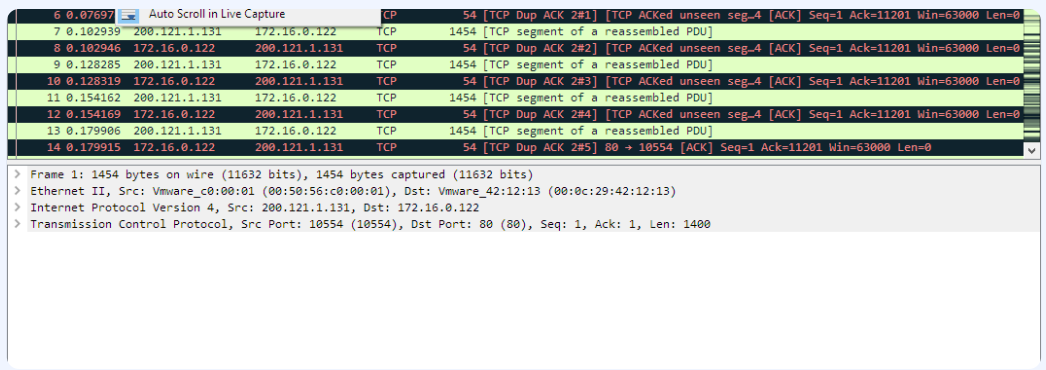
رسوم I/O: تحديد زيادة غير طبيعية في حركة المرور

GeoIP: تحديد مصادر الهجمات الجغرافية

تحليل التوقيت: تحديد أنماط تكرار الهجمات

تحليل البروتوكول: تحديد البروتوكولات المستهدفة

مستوى إكمال التحليل: 65%



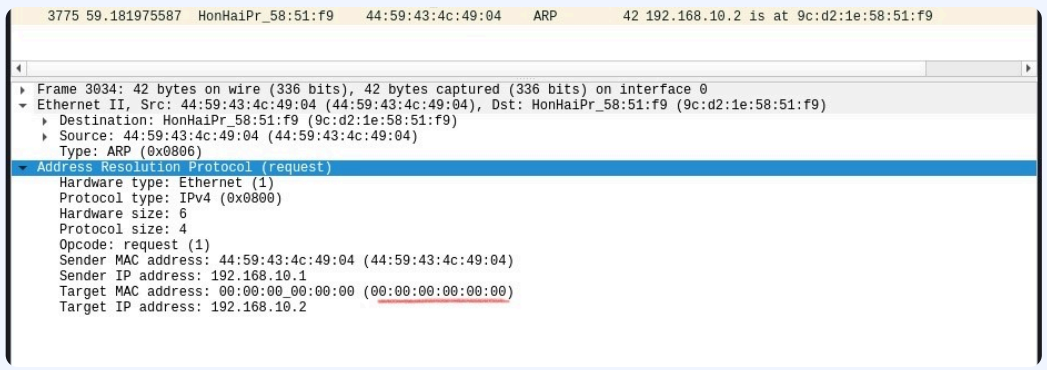
مهمة عملية

تحميل ملف PCAP: قم بتحميل ملف التقاط شبكة يحتوي على هجوم

تحليل الحزم: استخدم الفلاتر لتحديد نوع الهجوم

إنشاء رسوم بيانية: استخدم I/O Graph لتحليل نمط الهجوم

تقرير النتائج: قم بإعداد تقرير يحدد نوع الهجوم ومصدره



قضية عملية 3: تحليل بروتوكولات الشبكة

دراسة متعمقة لبروتوكولات TCP/IP و HTTP/DNS وتحليل سلوكها في ظروف مختلفة

بروتوكولات الشبكة الرئيسية

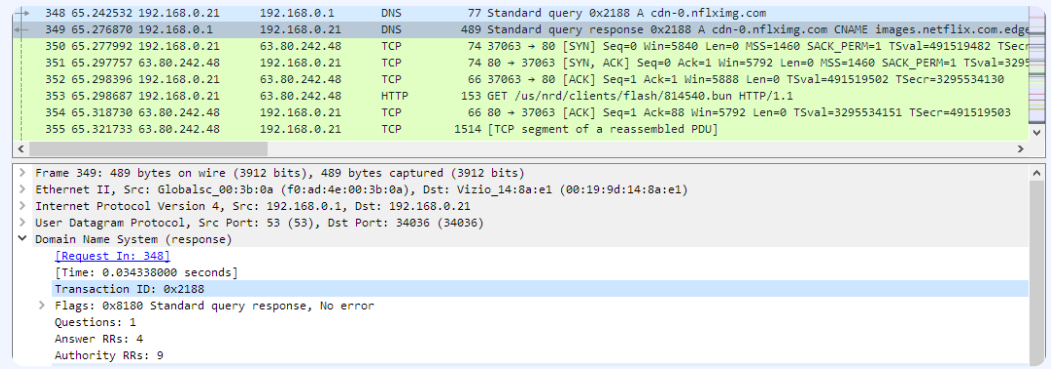
TCP IP HTTP DNS UDP ICMP ARP TLS

TCP: بروتوكول التحكم في الإرسال - موثوقية وموجه الاتصال

IP: بروتوكول الإنترنت - توجيه الحزم وعنونة الشبكة

HTTP: بروتوكول نقل النص التشعبي - طلبات واستجابات الويب

DNS: نظام أسماء النطاقات - ترجمة النطاقات إلى عناوين IP



فلاتر تحليل البروتوكولات

تحليل مصافحة TCP

```
tcp.flags.syn == 1 || tcp.flags.ack == 1
```

كشف إعادة إرسال TCP

```
tcp.analysis.retransmission
```

تحليل طلبات HTTP

```
"http.request.method == "GET
```

تحليل استعلامات DNS

```
dns.qry.type == 1 && dns.flags.response == 0
```

كشف أخطاء البروتوكول

```
tcp.analysis.flags || icmp.type == 3
```

تحليل سلوك البروتوكولات

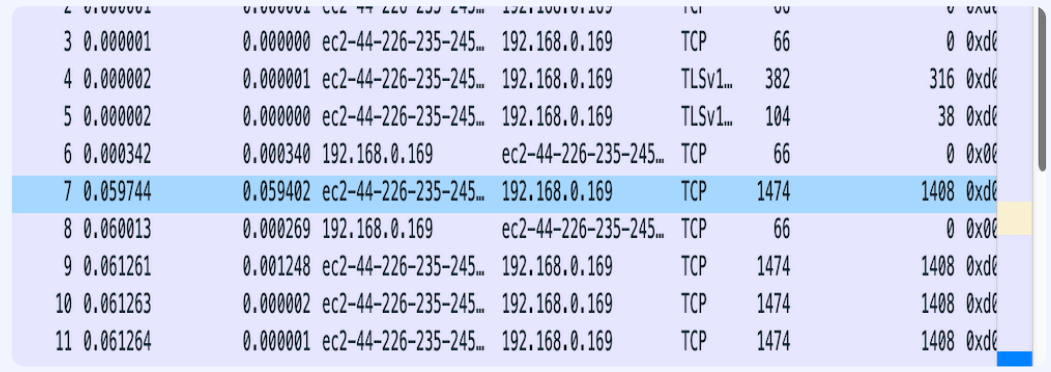
زمن الاستجابة: قياس زمن استجابة DNS و HTTP

الضغط: تحليل استخدام ضغط HTTP

التشفير: تحليل اتصالات TLS/SSL

الأداء: مقارنة أداء TCP مقابل UDP

مستوى إكمال التحليل: 80%



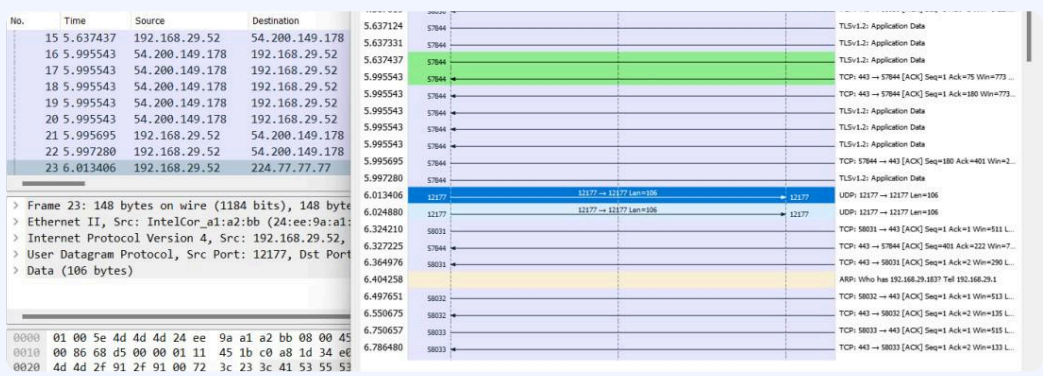
مهمة عملية

تحميل ملف PCAP: قم بتحميل ملف التقاط شبكة

تطبيق الفلاتر: استخدم فلاتر البروتوكولات

تحليل الأداء: قارن أداء البروتوكولات المختلفة

تقرير النتائج: قم بإعداد تقرير بتحليل البروتوكولات



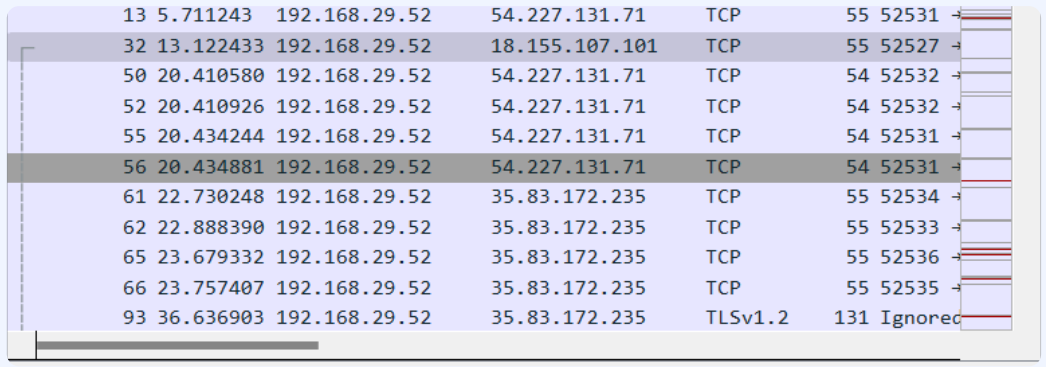
قضية عملية 4: استكشاف أخطاء الاتصال وتشخيصها

استخدام Wireshark لتشخيص مشاكل الاتصال وفقدان الحزم وإعادة الإرسال

أنواع مشاكل الاتصال الشائعة

فقدان الحزم | إعادة الإرسال | تأخير الاستجابة | انقطاع الاتصال | ازدحام الشبكة

- **فقدان الحزم:** حزم تصل متأخرة أو لا تصل على الإطلاق
- **إعادة الإرسال:** إرسال نفس الحزمة مرة أخرى
- **تأخير الاستجابة:** زمن استجابة أعلى من الطبيعي
- **انقطاع الاتصال:** انقطاع مفاجئ في الاتصال



فلاتر تشخيص المشاكل

كشف إعادة الإرسال

```
tcp.analysis.retransmission
```

كشف فقدان الحزم

```
tcp.analysis.lost_segment
```

كشف التأخير

```
frame.time_delta > 0.1
```

كشف أخطاء TCP

```
tcp.analysis.flags
```

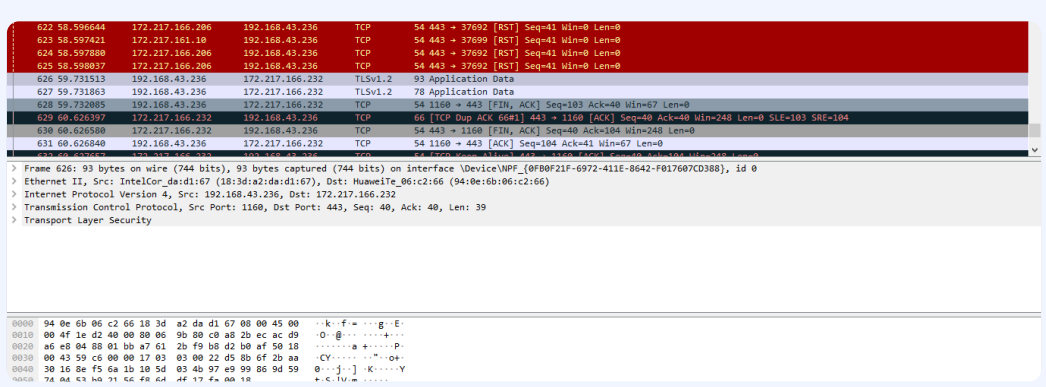
كشف الازدحام

```
tcp.window_size < 1000
```

أدوات التشخيص المتقدمة

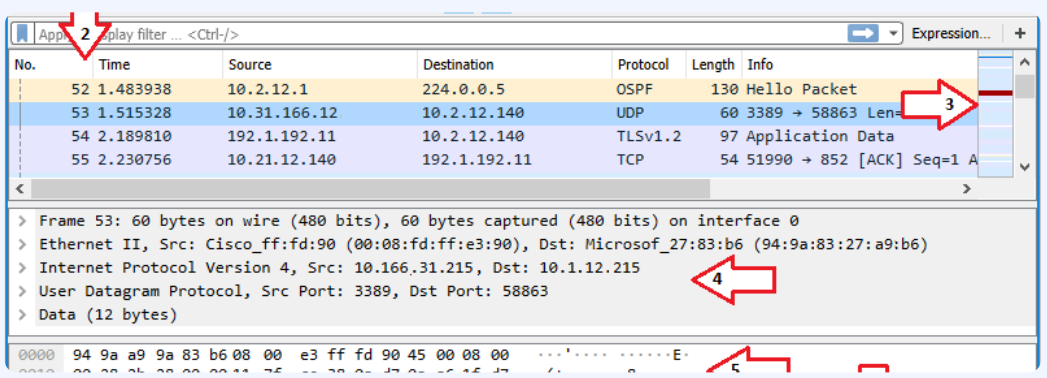
- **رسوم I/O:** تحليل أنماط حركة المرور
- **متابعة التدفق:** تحليل اتصالات TCP كاملة
- **إحصائيات نقطة النهاية:** تحديد الأجهزة النشطة
- **معلومات الخبير:** تحديد المشاكل المحتملة

مستوى إكمال التشخيص: 70%



مهمة عملية

- **تحميل ملف PCAP:** قم بتحميل ملف التقاط شبكة به مشاكل
- **تشخيص المشاكل:** استخدم الفلاتر لكشف المشاكل
- **تحليل الأداء:** استخدم الأدوات لتحليل الأداء
- **تقرير النتائج:** قم بإعداد تقرير بالتشخيص والحلول



قضية عملية 5: تحليل حركة المرور المشفرة

تقنيات فك تشفير TLS/SSL وتحليل حركة المرور المشفرة باستخدام Wireshark

بروتوكولات التشفير الشائعة

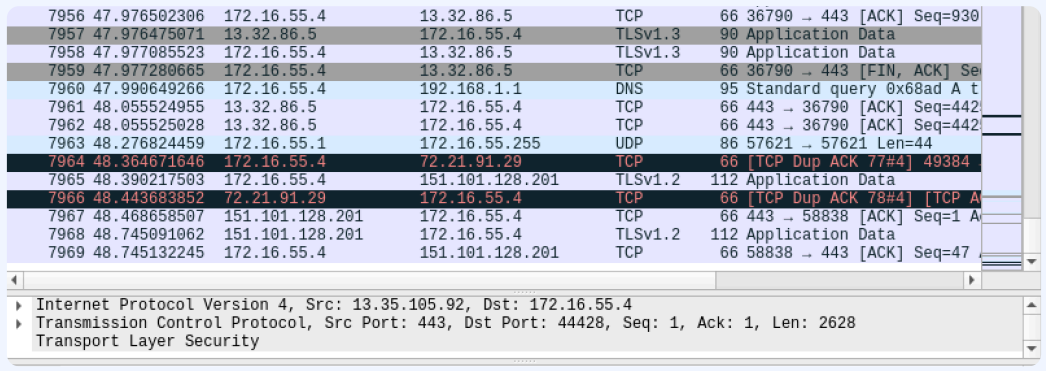
TLS 1.3 | TLS 1.2 | SSL 3.0 | HTTPS | FTPS | SSH

TLS/SSL: بروتوكولات تأمين طبقة النقل

المفاتيح: مفاتيح متناظرة وغير متناظرة

الشهادات: شهادات X.509 للتحقق من الهوية

مصافحة TLS: عملية التفاوض على خوارزمية التشفير



تقنيات فك التشفير

استخدام مفتاح الخادم الخاص

```
Edit → Preferences → Protocols → SSL → RSA Keys list
```

ملف سجل مفاتيح الجلسة

```
SSLKEYLOGFILE=~/sslkeylogfile.log
```

إعداد Wireshark لفك التشفير

```
Edit → Preferences → Protocols → SSL → (Pre)-Master-Secret log filename
```

فلتر حركة المرور المشفرة

```
ssl || tls
```

متابعة تدفق SSL

```
Analyze → Follow → SSL Stream
```

خطوات تحليل التشفير

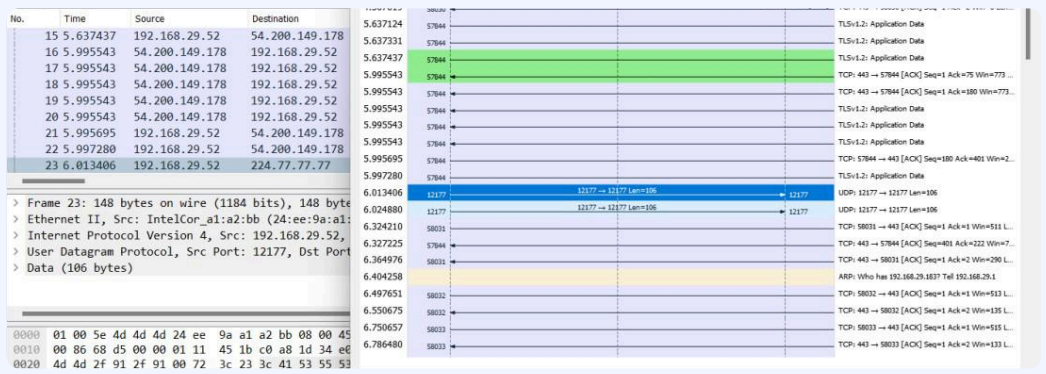
إعداد البيئة: تكوين متغير البيئة SSLKEYLOGFILE

إعادة تشغيل المتصفح: إعادة تشغيل المتصفح بعد الإعداد

بدء الالتقاط: بدء التقاط الحزم في Wireshark

تحليل الجلسات: عرض البيانات بعد فك التشفير

مستوى إكمال التحليل: 85%



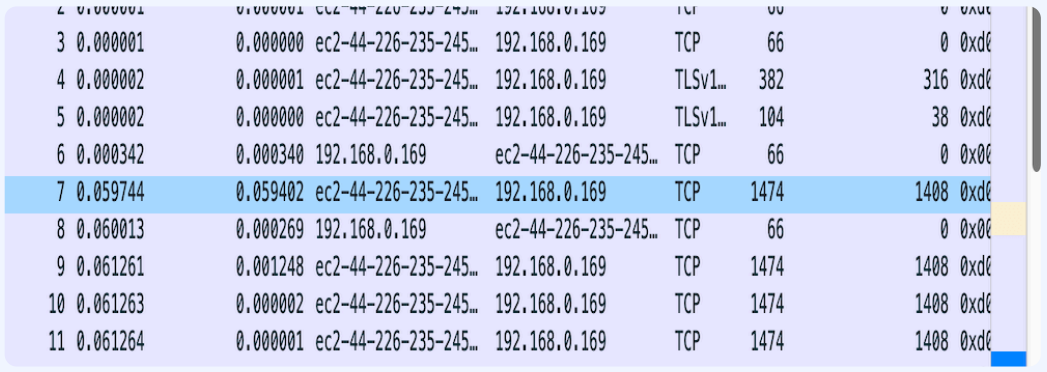
مهمة عملية

إعداد البيئة: تكوين متغير البيئة SSLKEYLOGFILE

إعداد Wireshark: تكوين Wireshark لاستخدام ملف السجل

التقاط الجلسات: التقاط حركة مرور HTTPS

تحليل النتائج: تحليل البيانات بعد فك التشفير



قضية عملية 6: تحليل سلوك التطبيقات

استخدام Wireshark لتحليل حركة مرور التطبيقات وتحديد مشاكل الأداء والأخطاء

أنواع التطبيقات المشتركة

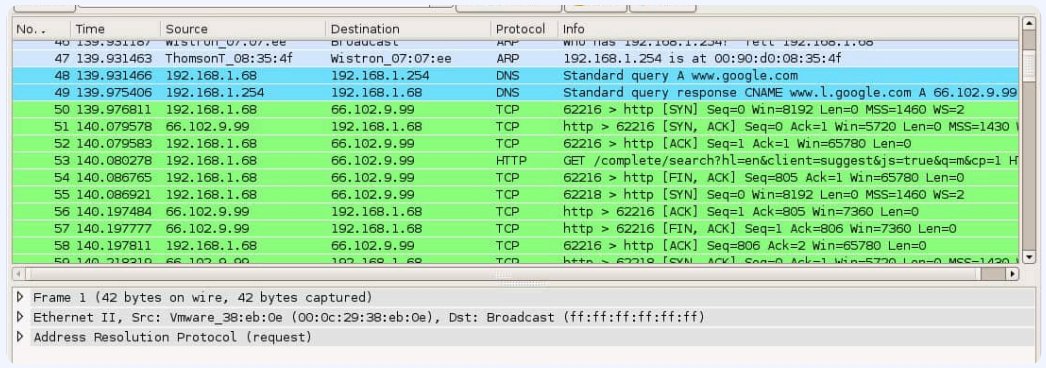
تطبيقات الويب | قواعد البيانات | البريد الإلكتروني | نقل الملفات | بث الفيديو | الدردشة

تطبيقات الويب: HTTP/HTTPS، REST APIs

قواعد البيانات: MySQL، PostgreSQL، MongoDB

البريد الإلكتروني: SMTP، POP3، IMAP

نقل الملفات: FTP، SFTP، SMB



فلاتر تحليل التطبيقات

تحليل حركة مرور HTTP

```
http.request.method == "GET" ||
"http.request.method == "POST
```

تحليل استعلامات قاعدة البيانات

```
mysql || postgres || tds
```

تحليل البريد الإلكتروني

```
smtp || pop || imap
```

تحليل نقل الملفات

```
ftp || sftp || smb
```

تحليل أداء التطبيق

```
tcp.time_delta > 0.1
```

تحليل مشاكل الأداء

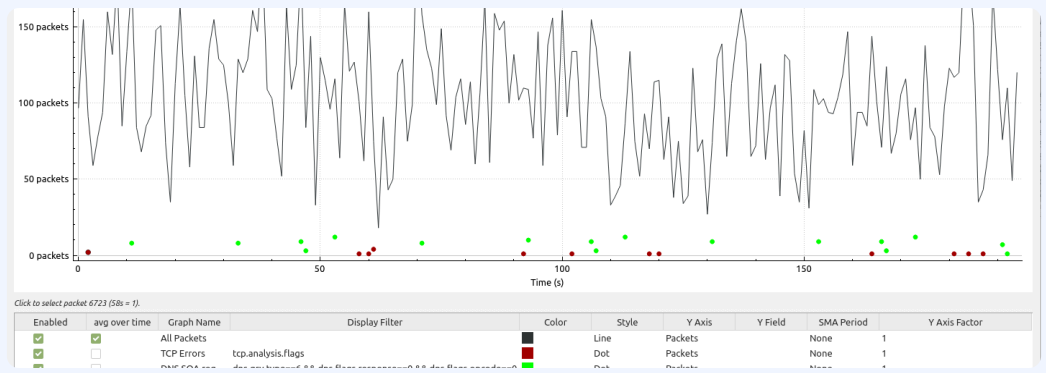
زمن الاستجابة: قياس زمن استجابة التطبيق

الأخطاء: تحديد أخطاء التطبيق والشبكة

الضغط: تحليل استخدام ضغط البيانات

الاتصالات: تحليل عدد الاتصالات المتزامنة

مستوى إكمال التحليل: 75%



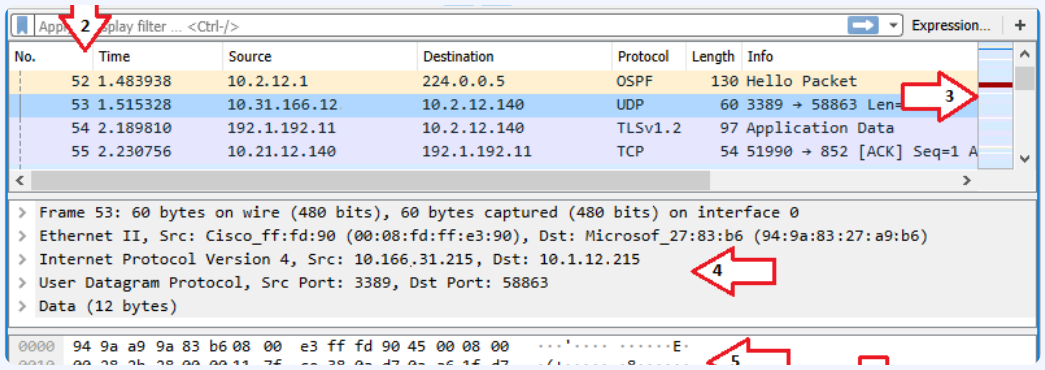
مهمة عملية

تحميل ملف PCAP: قم بتحميل ملف التقاط شبكة

تطبيق الفلاتر: استخدم فلاتر التطبيقات

تحليل الأداء: قسّم زمن استجابة التطبيق

تقرير النتائج: قم بإعداد تقرير بتحليل التطبيق



قضية عملية 7: تحليل الشبكات اللاسلكية

استخدام Wireshark لتحليل حركة مرور الشبكات اللاسلكية وكشف نقاط الضعف الأمنية

بروتوكولات الشبكات اللاسلكية

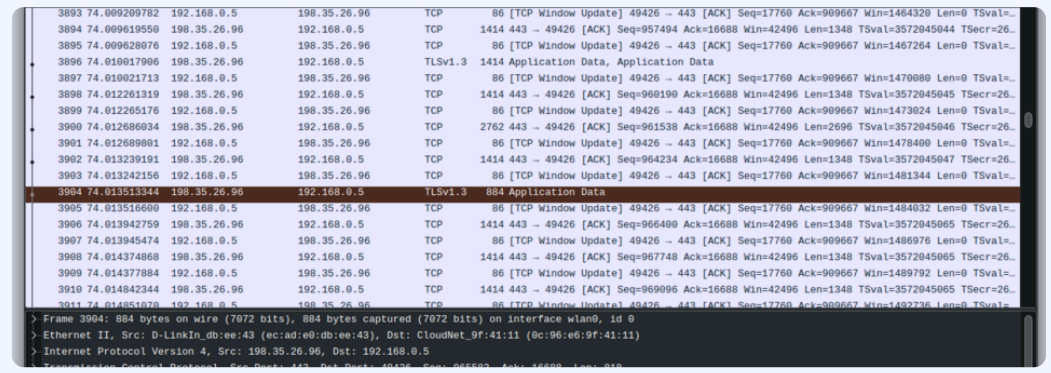
802.11 WEP WPA WPA2 WPA3 WPS

802.11: معايير الشبكات اللاسلكية

بروتوكولات التشفير: WEP، WPA، WPA2، WPA3

WPS: إعداد Wi-Fi المحمي

أنواع الحزم: إطارات التحكم، البيانات، الإدارة



فلاتر تحليل الشبكات اللاسلكية

فلتر حزم 802.11

```
wlan
```

فلتر حزم WPA/WPA2

```
wlan.wpa || wlan.rsn
```

فلتر نقاط الوصول

```
wlan.fc.type_subtype == 0x08
```

فلتر هجمات Deauthentication

```
wlan.fc.type_subtype == 0x0c
```

فلتر إشارات الاكتشاف

```
wlan.fc.type_subtype == 0x04
```

كشف نقاط الضعف الأمنية

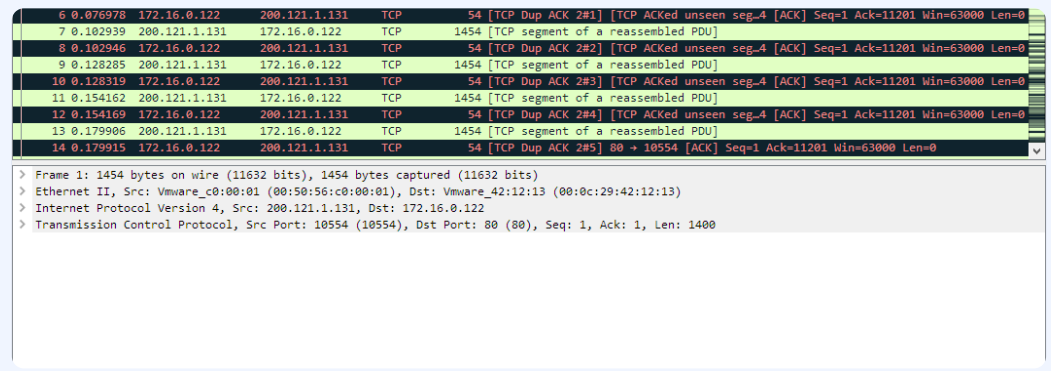
شبكات مفتوحة: كشف الشبكات غير المشفرة

هجمات Evil Twin: كشف نقاط وصول مزيفة

هجمات Deauth: كشف محاولات قطع الاتصال

ثغرات WPS: كشف نقاط الضعف في WPS

مستوى إكمال التحليل: 80%



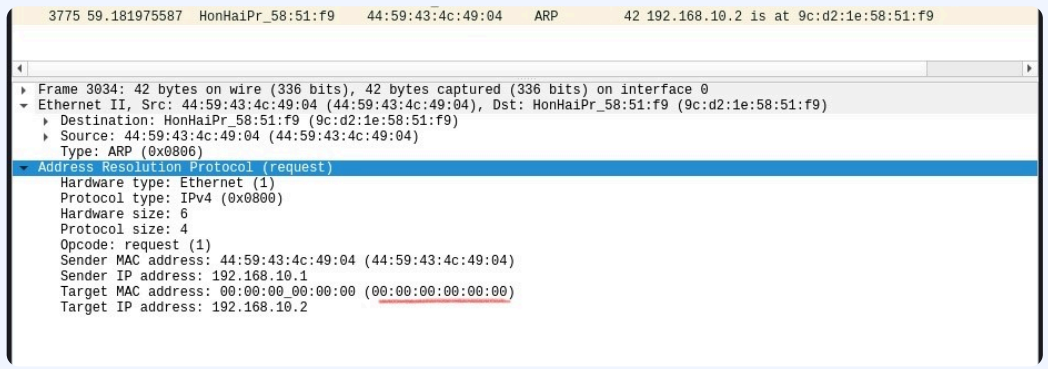
مهمة عملية

تحميل ملف PCAP: قم بتحميل ملف التقاط شبكة لاسلكية

تطبيق الفلاتر: استخدم فلاتر الشبكات اللاسلكية

كشف الثغرات: حدد نقاط الضعف الأمنية

تقرير النتائج: قم بإعداد تقرير بالتحليل والتوصيات



قضية عملية 8: تحليل حركة المرور الصوتية والفيديو (VoIP)

استخدام Wireshark لتحليل حركة مرور VoIP وتحديد مشاكل الجودة والأداء

بروتوكولات VoIP الرئيسية

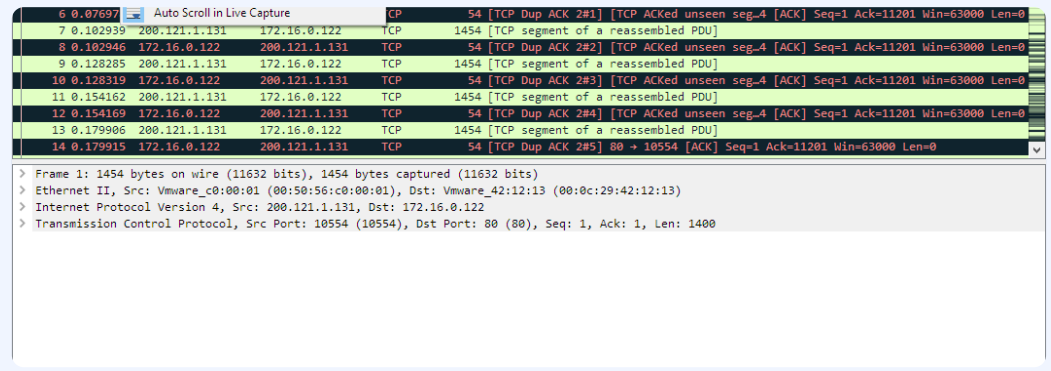
SIP | RTP | RTCP | H.323 | MGCP | Skinny

SIP: بروتوكول بدء الجلسة - إدارة المكالمات

RTP: بروتوكول النقل في الوقت الفعلي - نقل الصوت/الفيديو

RTCP: بروتوكول التحكم في RTP - مراقبة الجودة

H.323: مجموعة بروتوكولات للمؤتمرات الصوتية والمرئية



فلاتر تحليل VoIP

فلتر حزم SIP

```
sip
```

فلتر حزم RTP

```
rtp
```

فلتر حزم RTCP

```
rtcp
```

فلتر مكالمات SIP

```
"sip.Method == "INVITE
```

فلتر مشاكل RTP

```
rtp.ssrc || rtp.seq || rtp.timestamp
```

تحليل جودة VoIP

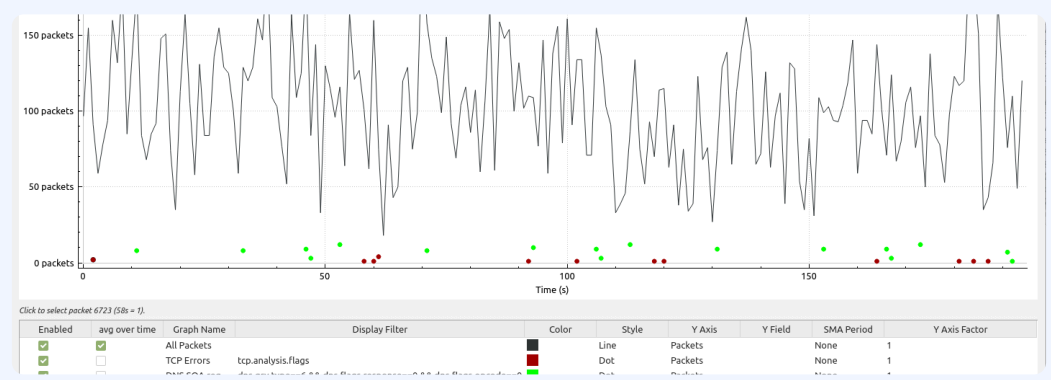
MOS: متوسط رأي المستخدم - قياس جودة الصوت

زمن الاستجابة: قياس التأخير في نقل الصوت

الاهتزاز: قياس تباين زمن الوصول للحزم

فقدان الحزم: حساب نسبة الحزم المفقودة

مستوى إكمال التحليل: 75%



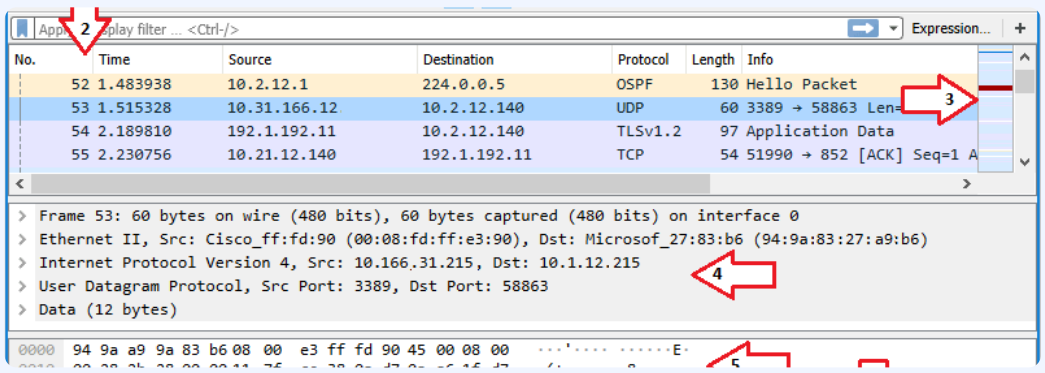
مهمة عملية

تحميل ملف PCAP: قم بتحميل ملف التقاط VoIP

تطبيق الفلاتر: استخدم فلاتر SIP و RTP

تحليل الجودة: استخدم أدوات تحليل RTP

تقرير النتائج: قم بإعداد تقرير بجودة الاتصال



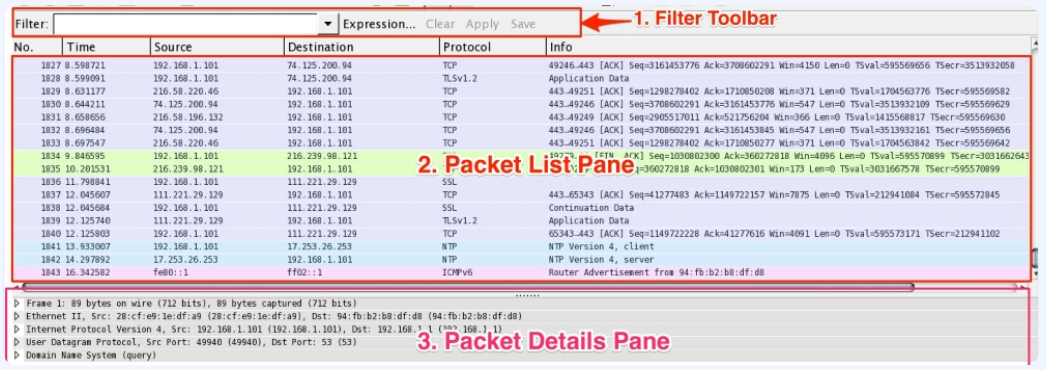
قضية عملية 9: استخراج البيانات والملفات من حزم الشبكة

استخدام Wireshark لاستخراج الملفات والبيانات من حزم الشبكة وتحليلها

أنواع الملفات القابلة للاستخراج

صور | مستندات | ملفات تنفيذية | ملفات وسائط | أرشيف | ملفات ضارة

- **الصور:** JPEG، PNG، GIF، SVG
- **المستندات:** PDF، DOCX، XLSX، PPTX
- **الملفات التنفيذية:** EXE، DLL، APK
- **الأرشيف:** ZIP، RAR، TAR، 7z



أدوات استخراج الملفات

استخراج كائنات HTTP

```
File → Export Objects → HTTP...
```

استخراج ملفات SMB

```
File → Export Objects → SMB...
```

استخراج مرفقات البريد

```
File → Export Objects → IMAP...
```

فلتر الملفات المستخرجة

```
"http.content_type contains "image
```

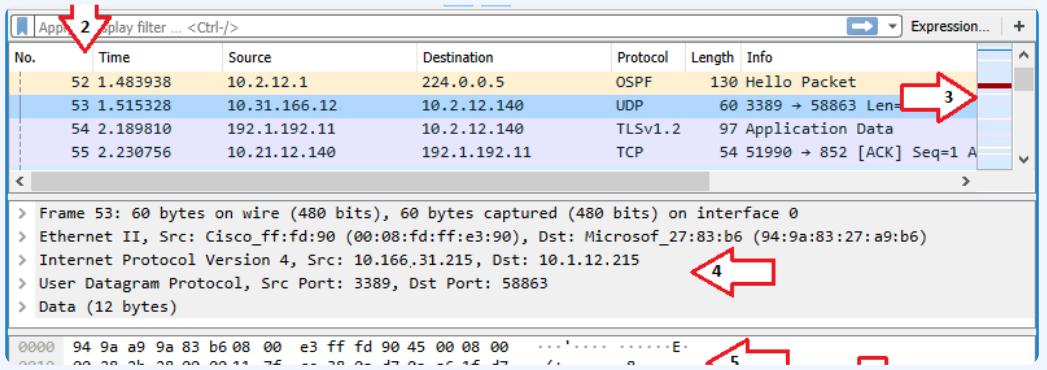
استخراج البيانات الثنائية

```
File → Export Packet Dissections → As CSV...
```

تقنيات تحليل الملفات المستخرجة

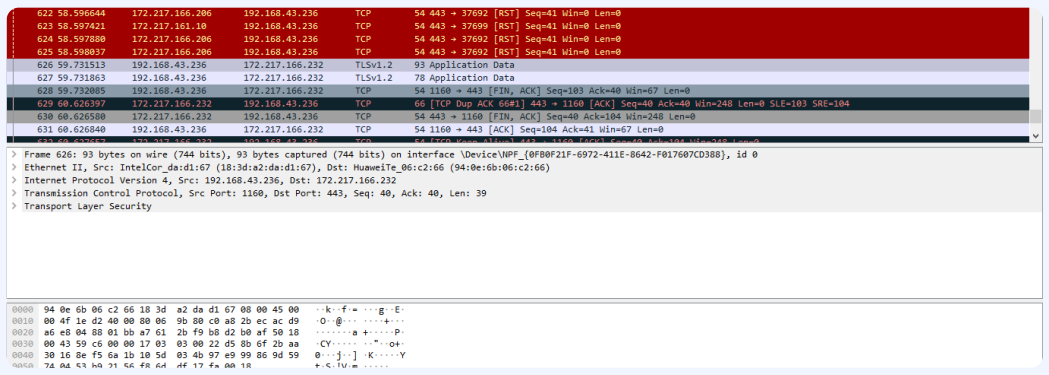
- **التحقق من سلامة الملف:** حساب تجزئة MD5/SHA
- **كشف البرامج الضارة:** فحص الملفات باستخدام مكافحة الفيروسات
- **التحليل الثنائي:** فحص محتوى الملفات الثنائية
- **تحليل البيانات الوصفية:** استخراج معلومات التعريف

مستوى إكمال التحليل: 85%



مهمة عملية

- **تحميل ملف PCAP:** قم بتحميل ملف التقاط شبكة
- **تطبيق الفلاتر:** استخدم فلاتر لتحديد الملفات
- **استخراج الملفات:** استخدم أدوات الاستخراج
- **تحليل النتائج:** قم بتحليل الملفات المستخرجة



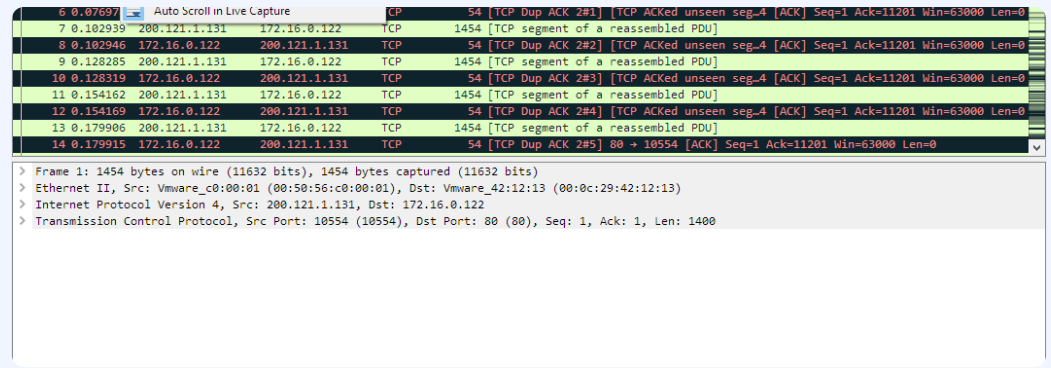
قضية عملية 10: تحقيق أمني متقدم

استخدام Wireshark في التحقيقات الأمنية المتقدمة وكشف التهديدات المعقدة وتحليل الهجمات المستمرة

أنواع التهديدات الأمنية المتقدمة

APT | هجمات صفرية | برامج فدية | هجمات التصيد | اختراق البيانات | هجمات DDoS

- **APT:** التهديدات المستمرة المتقدمة
- **هجمات صفرية:** استغلال ثغرات غير معروفة
- **برامج فدية:** تشفير الملفات وطلب فدية
- **هجمات التصيد:** انتحال هوية موثوقة



فلاتر التحقيق الأمني

كشف حركة المرور المشبوهة

```
frame.time_delta < 0.01 && frame.len > 1000
```

كشف محاولات الاتصال المشبوهة

```
tcp.flags.syn == 1 && tcp.flags.ack == 0
```

كشف أنشطة البرامج الضارة

```
"dns.qry.name matches "(malicious|suspicious)
```

كشف تسريب البيانات

```
http contains "password" || http contains
""credit_card
```

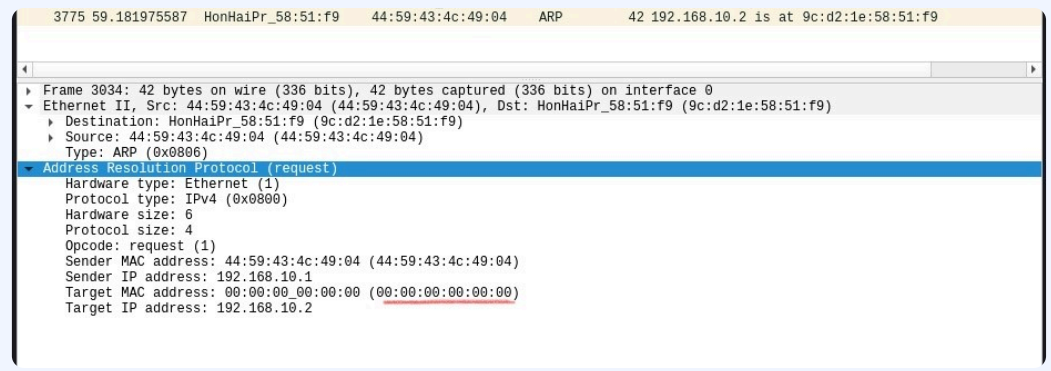
كشف الاتصالات غير المعتادة

```
ip.dst == 0.0.0.0/0 && tcp.port > 10000
```

تقنيات التحليل المتقدمة

- **تحليل السلوك:** تحديد أنماط السلوك غير المعتادة
- **تحليل الارتباطات:** ربط الأحداث المختلفة معاً
- **تحليل البصمات:** تحديد بصمات الهجمات المعروفة
- **التحليل الزمني:** تحليل تسلسل الأحداث الزمني

مستوى إكمال التحقيق: 90%



مهمة عملية

- **تحميل ملف PCAP:** قم بتحميل ملف التقاط شبكة بهجوم معقد
- **تطبيق الفلاتر:** استخدم فلاتر التحقيق الأمني
- **تحليل الهجوم:** حدد نوع الهجوم وأساليبه
- **تقرير التحقيق:** قم بإعداد تقرير تحقيق أمني شامل