CYBER DEFENSE

❖ حسین ملک زاده

مشاور و تحلیل گر ارشد امنیت سایبری

کارشناس ارشد امنیت اطلاعات ازدانشگاه Sapienza Universityرم – ایتالیا

مدرس و عضو هیات علمی دانشگاه بین المللی نورث وست Northwest International University

مدرس و عضو هیات علمی دانشگاه نیوجرسی New Jersey International Open University

مدرس و عضو هیات علمی موسسه دانشگاهی DEI Institute - Online Universityآفریقا

دارای مدرک دکترا مدیریت امنیت سایبری DBA - Cyber Security Management از دانشگاه بین المللی نورث وست

ممیز و سرممیز امنیت اطلاعات ISMS ISO27001-2013

دارای مدارک سطح عالی امنیت اطلاعات CISSP , CISA

دارای مدرک مشاور ارشد امنیت سیستمی SSCP

طراح – مشاور و مجری پروژه¬های شبکه و امنیت اطلاعات ISMS , SOC , NOC

دارای بیش از ۲۴ سال سابقه آموزشی – اجرایی و مدیریتی درزمینه پروژه¬های شبکه و امنیت در داخل و خارج از کشور

مدرس دوره¬های تخصصی شبکه و امنیت با بیش از دوازده هزارساعت تدریس درموسسات داخلی و بین المللی

دارای تحصیلات و مدارک بین المللی :

MCSE , CCNA ,CCNA Security , CCNP , CEH , CISSP , CWNA , ISMS , SSCP, GSNA

عضوانجمن مهندسین کامپیوتر و فناوری آمریکا IEEE , ACM

مولف کتاب هنر هک کردن انسان در حوزه امنیت در مهندسی اجتماعی Social engineering

www.Hosseinmalekzadeh.com

Mobile: 09153133217

E-mail: Hoseeinmalekzadeh@Gmail.com

Telegram Channel : https://t.me/HosseinMalekzadeh

http://www.linkedin.com/in/hosseinmalekzadeh

@HOSSEINMALEKZADEH2015

@HOSSEINMALEKZADEH

By. Hossein Malekzadeh

Cyber Security Consultant and Manager

www.Hosseinmalekzadeh.com

Mobile : 09153133217

نقشه شبکه سازمان (دفتر مرکزی)

سناریوی سازمان

یک سازمان متوسط با حدود ۵۰۰ کارمند
دارای دفتر مرکزی و دو شعبه
خدمات اصلی سازمان شامل:

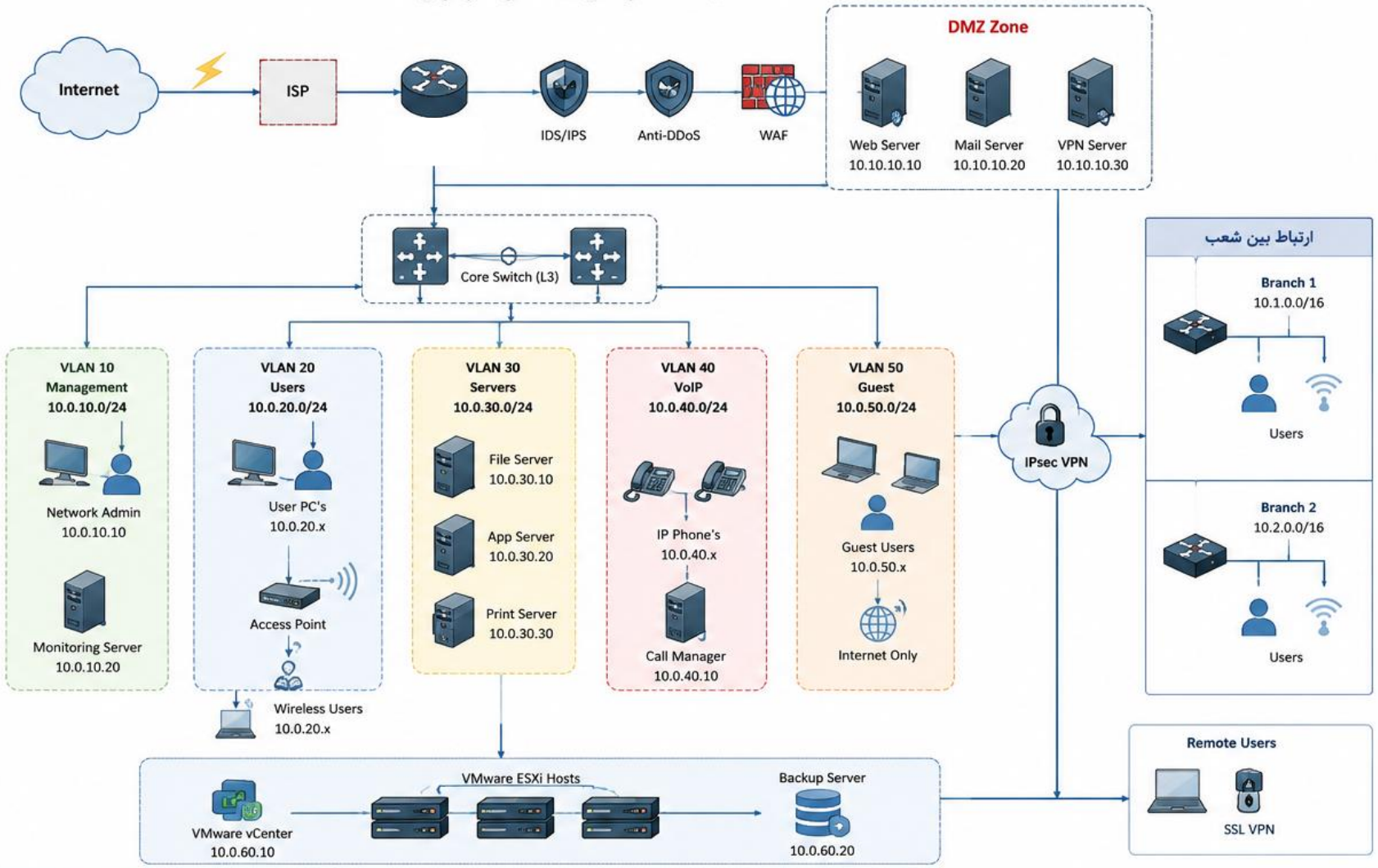
- سرویس های دایرکتوری (Active Directory)
- سرورهای فایل و پرینت
- سرور برنامه کاربردی تحت وب
- سیستم تلفنی تحت شبکه (VoIP)
- دسترسی کاربران به اینترنت
- ارتباط امن بین شعب از طریق VPN
- زیرساخت مجازی سازی با VMware

اهداف امنیتی

- حفاظت لایه به لایه از اطلاعات و سرویس ها
- جلوگیری از دسترسی غیرمجاز
- جلوگیری از حرکت جانبی مهاجم در شبکه
- مانیتورینگ و پاسخ به رخدادها
- پشتیبان گیری و تداوم کسب و کار

چالش ها / تهدیدات

- حملات اینترنتی (Brute Force, Exploit, DDoS)
- فیشینگ و مهندسی اجتماعی
- بدافزار و باج افزار
- تهدیدات داخلی و دسترسی بیش از حد
- نشت اطلاعات
- خرابی تجهیزات و از دسترس خارج شدن سرویس ها



راهنمای نمادها

اینترنت — کلاینت — فایروال / روتر
سیستم امنیتی — تلفن تحت شبکه — سوئیچ لایه ۳
دسترسی بی سیم — سرور

نکات طراحی امنیتی (Defense in Depth)

- لایه محیطی: فایروال, IDS/IPS, Anti-DDoS, WAF
- لایه شبکه: تقسیم بندی VLAN, Private VLAN, Private VLAN Security
- لایه سیستم: هاردنینگ سررورها و کلاینت ها، بروزرسانی Patch Management
- لایه هویت و دسترسی: Mtive Directory Security, Least Privilege Security
- لایه مانیتورینگ: جمع آوری و تحلیل لاگ ها در SIEM
- لایه داده: رمزنگاری: DLP, Backup منظم
- لایه پنجم پاسخ: Incident Response Plan و تمرین دوره ای

جدول آدرس دهی

VLAN	Network	Gateway	Description
10	10.0.10.0/24	10.0.10.1	Management
20	10.0.20.0/24	10.0.20.1	Users
30	10.0.30.0/24	10.0.30.1	Servers
40	10.0.40.0/24	10.0.40.1	VoIP
50	10.0.50.0/24	10.0.50.1	Guest
60	10.0.60.0/24	10.0.60.1	Virtualization/Backup
DMZ	10.10.10.0/24	10.10.10.1	DMZ Zone

- **پیدا کردن IPمهاجم**
- **سناریو:**
- یک سیستم Victim در حال دریافت ترافیک غیرعادی است.
- گام‌ها:
- Attacker اجرا می‌کند:
- ping 192.168.100.20
- **تحلیلگر در Wireshark باید:**

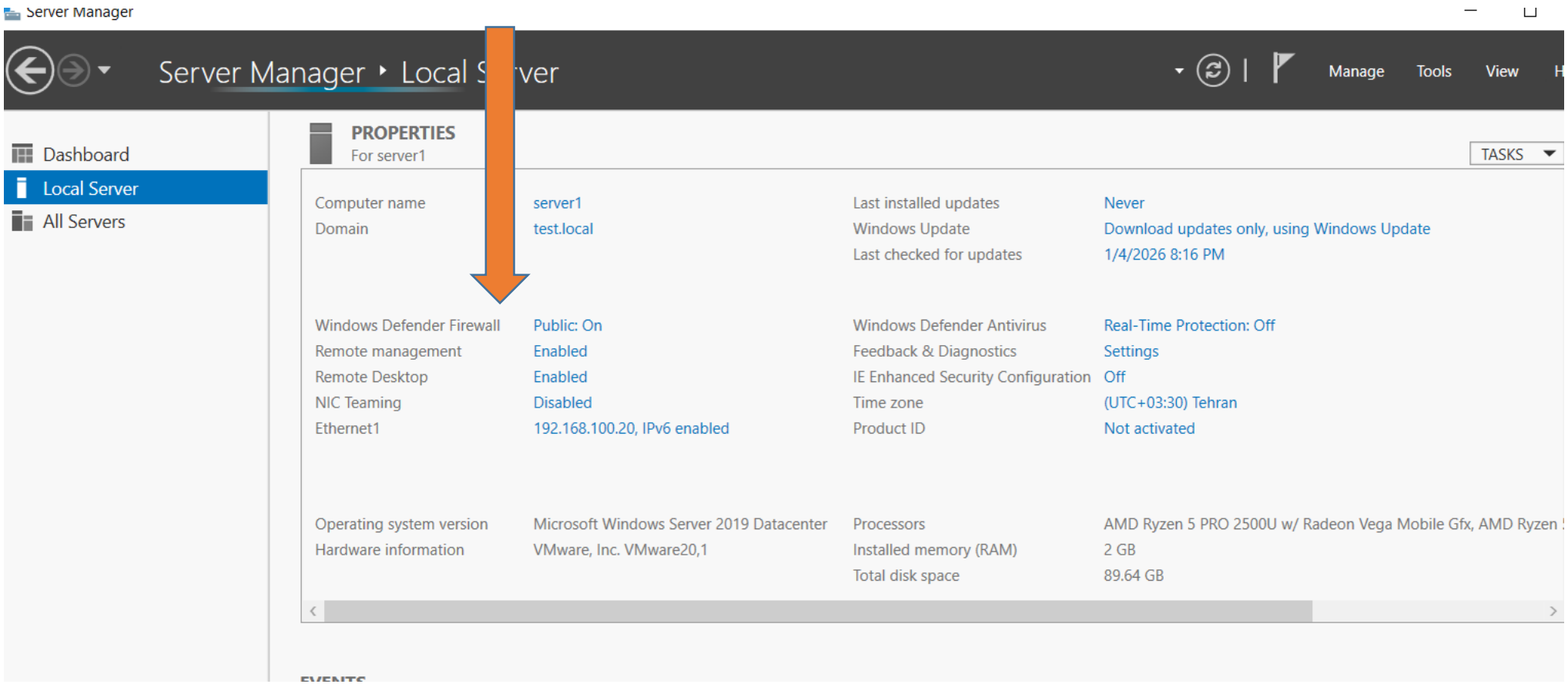
1. Packet ها را پیدا کند
2. Source IP را شناسایی کند

- فیلتر:

- icmp

- هدف تمرین:
- تشخیص:

- Attacker IP
- Victim IP



```
File  Actions  Edit  View  Help
┌──(hesam㉿kali)-[~]
└─$ sudo -s
[sudo] password for hesam:
┌──(root㉿kali)-[/home/hesam]
└─# ping 192.168.100.20
PING 192.168.100.20 (192.168.100.20) 56(84) bytes of data.
```

icmp

No.	Time	Source	Destination	Protocol	Length	Info
8	3.332095	192.168.100.50	192.168.100.20	ICMP	98	Echo (ping) request id=0xec41, seq=55/14080, ttl=64 (no response found!)
10	4.355952	192.168.100.50	192.168.100.20	ICMP	98	Echo (ping) request id=0xec41, seq=56/14336, ttl=64 (no response found!)
15	5.380808	192.168.100.50	192.168.100.20	ICMP	98	Echo (ping) request id=0xec41, seq=57/14592, ttl=64 (no response found!)
17	6.404237	192.168.100.50	192.168.100.20	ICMP	98	Echo (ping) request id=0xec41, seq=58/14848, ttl=64 (no response found!)
18	7.428205	192.168.100.50	192.168.100.20	ICMP	98	Echo (ping) request id=0xec41, seq=59/15104, ttl=64 (no response found!)
22	8.456324	192.168.100.50	192.168.100.20	ICMP	98	Echo (ping) request id=0xec41, seq=60/15360, ttl=64 (no response found!)
24	9.476060	192.168.100.50	192.168.100.20	ICMP	98	Echo (ping) request id=0xec41, seq=61/15616, ttl=64 (no response found!)
27	10.501081	192.168.100.50	192.168.100.20	ICMP	98	Echo (ping) request id=0xec41, seq=62/15872, ttl=64 (no response found!)
28	11.524701	192.168.100.50	192.168.100.20	ICMP	98	Echo (ping) request id=0xec41, seq=63/16128, ttl=64 (no response found!)
29	12.547444	192.168.100.50	192.168.100.20	ICMP	98	Echo (ping) request id=0xec41, seq=64/16384, ttl=64 (no response found!)
30	13.572095	192.168.100.50	192.168.100.20	ICMP	98	Echo (ping) request id=0xec41, seq=65/16640, ttl=64 (no response found!)

```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Devi
> Ethernet II, Src: VMware_45:2d:24 (00:0c:29:45:2d:24), Dst: VMware_69:a3:77 (00:0c:29
> Internet Protocol Version 4, Src: 192.168.100.50, Dst: 192.168.100.20
> Internet Control Message Protocol

0000  00 0c 29 69 a3 77 00 0c  29 45 2d 24 08 00 45 00   ··)i·w·· )E-$··E·
0010  00 54 49 52 40 00 40 01  a7 bf c0 a8 64 32 c0 a8   ·TIR@·@· ····d2··
0020  64 14 08 00 62 ef ec 41  00 34 3e 5a 09 6a 00 00   d···b··A ·4>Z·j··
0030  00 00 9c 03 06 00 00 00  00 00 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

- مهاجم در حال اسکن پورت‌ها است.
- nmap 192.168.100.20
- تحلیلگر در Wireshark:
- فیلتر:
- tcp.flags.syn == 1 && tcp.flags.ack == 0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
458	300.496580	192.168.100.50	192.168.100.20	TCP	60	33550 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
459	300.496580	192.168.100.50	192.168.100.20	TCP	60	33550 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
460	300.496765	192.168.100.50	192.168.100.20	TCP	60	33550 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
461	300.496765	192.168.100.50	192.168.100.20	TCP	60	33550 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
463	300.497699	192.168.100.50	192.168.100.20	TCP	60	33550 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
464	300.497699	192.168.100.50	192.168.100.20	TCP	60	33550 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
465	300.497699	192.168.100.50	192.168.100.20	TCP	60	33550 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
466	300.497699	192.168.100.50	192.168.100.20	TCP	60	33550 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
467	300.497699	192.168.100.50	192.168.100.20	TCP	60	33550 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
468	300.497699	192.168.100.50	192.168.100.20	TCP	60	33550 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
472	300.501046	192.168.100.50	192.168.100.20	TCP	60	33550 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
473	300.501046	192.168.100.50	192.168.100.20	TCP	60	33550 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

```
> Frame 458: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \De
> Ethernet II, Src: VMware_45:2d:24 (00:0c:29:45:2d:24), Dst: VMware_69:a3:77 (00:0c:29
> Internet Protocol Version 4, Src: 192.168.100.50, Dst: 192.168.100.20
> Transmission Control Protocol, Src Port: 33550, Dst Port: 3306, Seq: 0, Len: 0

0000  00 0c 29 69 a3 77 00 0c  29 45 2d 24 08 00 45 00   ··)i·w·· )E-$··E·
0010  00 2c f4 02 00 00 35 06  48 32 c0 a8 64 32 c0 a8   ·,····5· H2··d2··
0020  64 14 83 0e 0c ea ad de  80 b0 00 00 00 00 60 02   d····· ·····`··
0030  04 00 8c 07 00 00 02 04  05 b4 00 00               ···· ····
```

- فیلتر زیر در **Wireshark** برای شناسایی تلاش‌های اولیه اتصال TCP (که اغلب در **Port Scan** دیده می‌شود) استفاده می‌شود:
- tcp.flags.syn == 1 && tcp.flags.ack == 0
- در پروتکل TCP چند **Flag** مهم وجود دارد که وضعیت اتصال را مشخص می‌کنند:

Flag	معنی
SYN	شروع اتصال
ACK	تایید دریافت
FIN	پایان اتصال
RST	ریست اتصال
PSH	ارسال فوری داده
URG	داده فوری

- برقراری اتصال TCP در سه مرحله انجام می‌شود:
- کلاینت درخواست اتصال می‌دهد.
- Client → Server
- **SYN**
- سرور پاسخ می‌دهد.
- Server → Client
- **SYN + ACK**
- کلاینت تایید می‌کند.
- Client → Server
- **ACK**

- فیلتر:
- tcp.flags.syn == 1
- یعنی:
- Packetدارای SYNاست
- tcp.flags.ack == 0
- ACKوجود ندارد
- **چرا این فیلتر برای SOCمهم است؟**
- در Port Scan مهاجم معمولاً هزاران اتصال اولیه ایجاد می‌کند.
- مثلاً ابزار nmap:

- nmap -sS 192.168.1.10

- این ابزار تعداد زیادی SYN Packet ارسال می‌کند.
- **بدون اینکه اتصال کامل شود.**

```
Nmap done: 1 IP address (1 host up) scanned in 17.42 seconds

┌──(root㉿kali)-[/home/hesam]
└─# nmap -sS 192.168.100.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-05-17 02:23 EDT
```

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

No.	Time	Source	Destination	Protocol	Length	Info
458	-899.775321	192.168.100.50	192.168.100.20	TCP	60	33550 → 3306 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
459	-899.775321	192.168.100.50	192.168.100.20	TCP	60	33550 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
460	-899.775136	192.168.100.50	192.168.100.20	TCP	60	33550 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
461	-899.775136	192.168.100.50	192.168.100.20	TCP	60	33550 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
463	-899.774202	192.168.100.50	192.168.100.20	TCP	60	33550 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
464	-899.774202	192.168.100.50	192.168.100.20	TCP	60	33550 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
465	-899.774202	192.168.100.50	192.168.100.20	TCP	60	33550 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
466	-899.774202	192.168.100.50	192.168.100.20	TCP	60	33550 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
467	-899.774202	192.168.100.50	192.168.100.20	TCP	60	33550 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
468	-899.774202	192.168.100.50	192.168.100.20	TCP	60	33550 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
472	-899.770855	192.168.100.50	192.168.100.20	TCP	60	33550 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
473	-899.770855	192.168.100.50	192.168.100.20	TCP	60	33550 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

```
> Frame 458: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \De
> Ethernet II, Src: VMware_45:2d:24 (00:0c:29:45:2d:24), Dst: VMware_69:a3:77 (00:0c:29

0000  00 0c 29 69 a3 77 00 0c  29 45 2d 24 08 00 45 00   ··)i·w·· )E-$··E
0010  00 2c f4 02 00 00 35 06  48 32 c0 a8 64 32 c0 a8   ·,····5· H2··d2··
```

- وقتی این فیلتر را اعمال کنید:
- tcp.flags.syn == 1 && tcp.flags.ack == 0
- Wireshark فقط نشان می‌دهد:
- TCP connection attempts
- یعنی:
- شروع اتصال‌ها
- SYN Scan
- تلاش برای اتصال

تحلیل DNS

- سناریو:
- کاربر یک دامنه را Resolve می‌کند.
- Victim اجرا می‌کند:
- nslookup google.com
- تحلیل در Wireshark:
- dns

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
79…	2828.492693	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x7b8d AAAA 2.debian.pool.ntp.org
79…	2833.496268	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xab89 A 2.debian.pool.ntp.org
79…	2833.496413	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x7b8d AAAA 2.debian.pool.ntp.org
79…	2838.504234	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x1880 A 3.debian.pool.ntp.org
79…	2838.504464	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xb59a AAAA 3.debian.pool.ntp.org
79…	2843.510343	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x1880 A 3.debian.pool.ntp.org
79…	2843.510679	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xb59a AAAA 3.debian.pool.ntp.org
79…	2848.517589	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x95ef A 0.debian.pool.ntp.org
79…	2848.517957	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xeaea AAAA 0.debian.pool.ntp.org
79…	2853.523980	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x95ef A 0.debian.pool.ntp.org
79…	2853.523980	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xeaea AAAA 0.debian.pool.ntp.org

```
> Frame 457: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \De
> Ethernet II, Src: VMware_45:2d:24 (00:0c:29:45:2d:24), Dst: HuaweiTechno_87:50:f1 (74
> Internet Protocol Version 4, Src: 192.168.100.50, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 52262, Dst Port: 53

0000  74 d2 1d 87 50 f1 00 0c  29 45 2d 24 08 00 45 00   t···P··· )E-
0010  00 43 be de 40 00 40 11  46 e1 c0 a8 64 32 08 08   ·C··@·@· F··
0020  08 08 cc 26 00 35 00 2f  7d c1 50 99 01 00 00 01   ···&·5·/ }·P
0030  00 00 00 00 00 00 01 31  06 64 65 62 69 61 6e 04   ······ 1·de
```

تحلیلگر باید ببیند:

Query

Response

Resolved IP

- این سه مورد مربوط به **فرآیند کامل DNS Resolution** هستند که در Wireshark می‌توان آن‌ها را دید.
- وقتی کلاینت می‌خواهد یک دامنه را به IP تبدیل کند، سه عنصر اصلی در ترافیک DNS دیده می‌شود:

- Query
- Response
- Resolved IP

- **DNS Query**
- **Query** درخواست کلاینت برای پیدا کردن IP یک دامنه است.
- مثال سناریو:
- کاربر در مرورگر می‌نویسد:
- google.com
- سیستم ابتدا باید IP این دامنه را پیدا کند، بنابراین یک درخواست DNS می‌فرستد.

- در Wireshark معمولاً چنین چیزی می‌بینید:
- Source: 192.168.1.10
- Destination: 8.8.8.8
- Protocol: DNS
- Info: Standard query A google.com
- **تحلیل:**
- **Source IP** → سیستم کاربر
- **Destination IP** → DNS Server
- **Query Type A** → درخواست IPv4

- **DNS Response**
- بعد از Query، سرور DNS پاسخ می‌دهد.
- در Wireshark می‌بینید
- Source: 8.8.8.8
- Destination: 192.168.1.10
- Protocol: DNS
- Info: Standard query response
- در داخل Packet بخش Answers دیده می‌شود.

Capturing from Ethernet1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
89…	3374.206306	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xcff1 AAAA 0.debian.pool.ntp.org
89…	3379.213224	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x0b2a A 1.debian.pool.ntp.org
89…	3379.213460	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xbb30 AAAA 1.debian.pool.ntp.org
89…	3384.219068	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x0b2a A 1.debian.pool.ntp.org
89…	3384.219459	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xbb30 AAAA 1.debian.pool.ntp.org
89…	3389.226609	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x2c45 A 2.debian.pool.ntp.org
89…	3389.226701	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x7cbd AAAA 2.debian.pool.ntp.org
89…	3394.232297	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x2c45 A 2.debian.pool.ntp.org
89…	3394.232589	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x7cbd AAAA 2.debian.pool.ntp.org
89…	3399.239117	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x61cf A 3.debian.pool.ntp.org
89…	3399.239457	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xd7c3 AAAA 3.debian.pool.ntp.org

```
> Frame 457: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \De
> Ethernet II, Src: VMware_45:2d:24 (00:0c:29:45:2d:24), Dst: HuaweiTechno_87:50:f1 (74
> Internet Protocol Version 4, Src: 192.168.100.50, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 52262, Dst Port: 53
v Domain Name System (query)
  > Transaction ID: 0x5099
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
```

```
0000  74 d2 1d 87 50 f1 00 0c  29 45 2d 24 08 00 45 00   t···P··· )E-$··E·
0010  00 43 be de 40 00 40 11  46 e1 c0 a8 64 32 08 08   ·C··@·@· F···d2··
0020  08 08 cc 26 00 35 00 2f  7d c1 50 99 01 00 00 01   ···&·5·/ }·P·····
0030  00 00 00 00 00 00 01 31  06 64 65 62 69 61 6e 04   ·******1 ·debian·
0040  70 6f 6f 6c 03 6e 74 70  03 6f 72 67 00 00 1c 00   pool·ntp ·org····
0050  01                                                 ·
```

- **Resolved IP**
- **Resolved IP** همان IP نهایی است که DNS برمی‌گرداند.
- در Wireshark در بخش زیر دیده می‌شود:
- Domain Name System
- Answers
- Name: google.com
- Address: 142.250.190.14
- این IP همان چیزی است که سیستم برای اتصال استفاده می‌کند.
- بعد از آن معمولاً ترافیک جدید شروع می‌شود

```
Nmap done: 1 IP address (1 host up) scanned in 17.58 seconds

┌──(root㉿kali)-[/home/hesam]
└─# nslookup google.com
;; communications error to 8.8.8.8#53: timed out
;; communications error to 8.8.8.8#53: timed out
;; communications error to 8.8.8.8#53: timed out
;; no servers could be reached

┌──(root㉿kali)-[/home/hesam]
└─#
```

- مثال رفتار مشکوک:

- ajd83js82kdn2.domain.com
- x82kdn2kdd.domain.com
- 82kdkd92kd.domain.com

- این می‌تواند نشانه:

- DNS Tunneling

- **فیلتر کردن DNS**
- ابتدا فقط DNS را ببینید.
- **در Wireshark:**
- فقط Query و Response های DNS نمایش داده می‌شوند.

Capturing from Ethernet1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

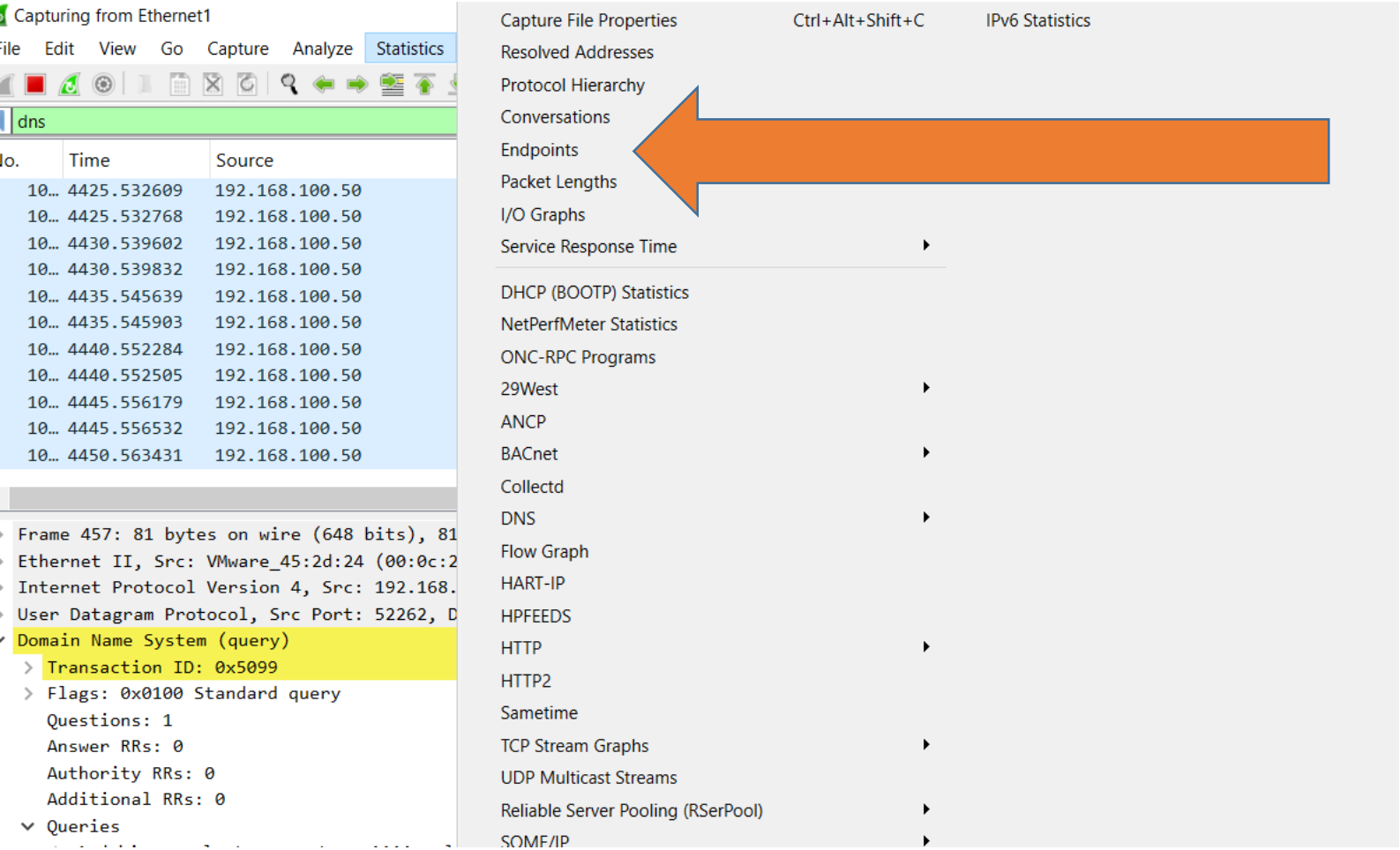
No.	Time	Source	Destination	Protocol	Length	Info
10…	4315.375642	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x5a5e AAAA 2.debian.pool.ntp.org
10…	4320.380874	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x779a A 3.debian.pool.ntp.org
10…	4320.380874	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x5a9c AAAA 3.debian.pool.ntp.org
10…	4325.386795	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x779a A 3.debian.pool.ntp.org
10…	4325.387431	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x5a9c AAAA 3.debian.pool.ntp.org
10…	4330.394191	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x083a A 0.debian.pool.ntp.org
10…	4330.394338	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x2801 AAAA 0.debian.pool.ntp.org
10…	4335.399897	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x083a A 0.debian.pool.ntp.org
10…	4335.400224	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x2801 AAAA 0.debian.pool.ntp.org
10…	4340.406572	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xeb93 A 1.debian.pool.ntp.org
10…	4340.406792	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xfa96 AAAA 1.debian.pool.ntp.org

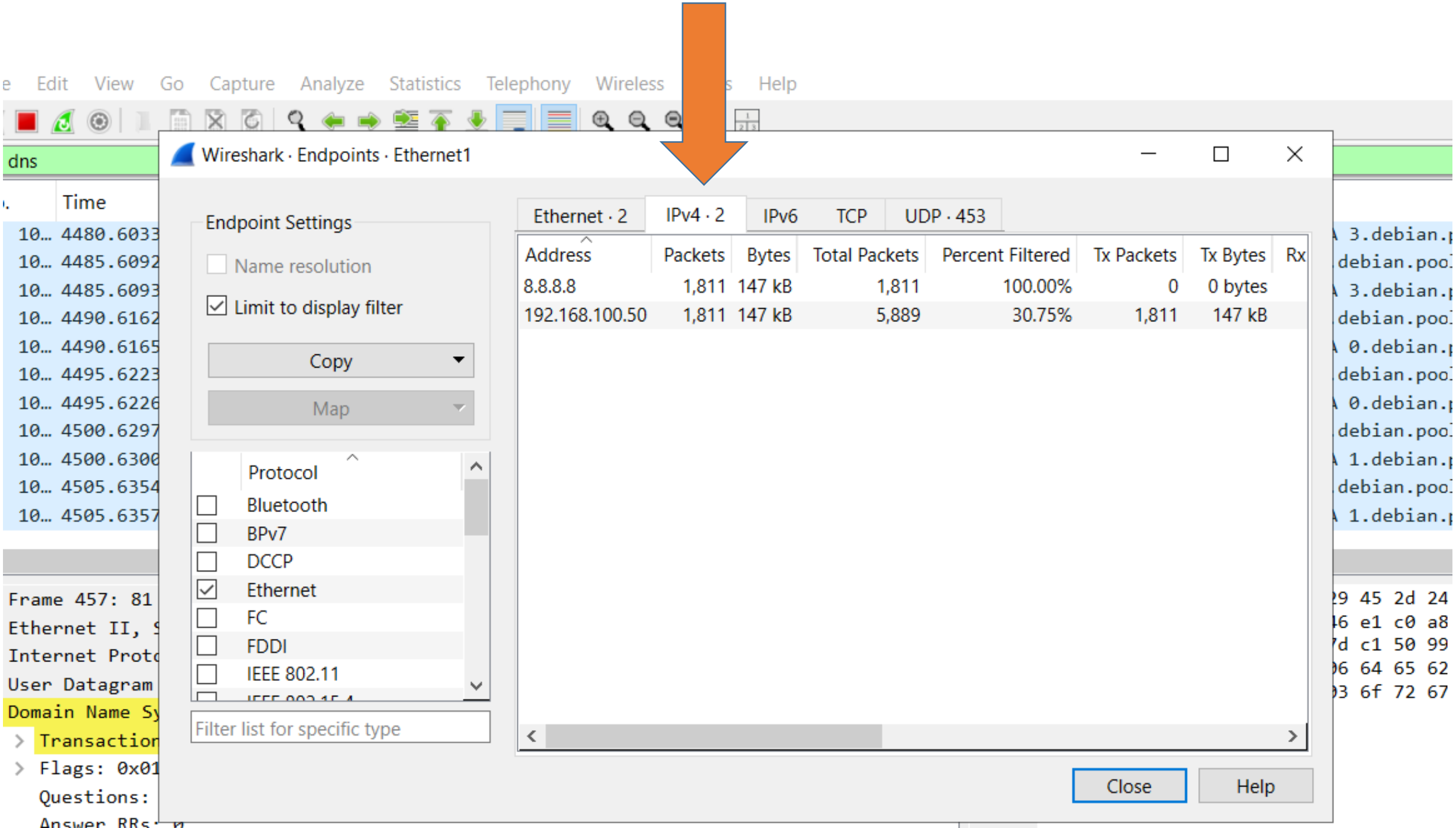
```
> Frame 457: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \De
> Ethernet II, Src: VMware_45:2d:24 (00:0c:29:45:2d:24), Dst: HuaweiTechno_87:50:f1 (74
> Internet Protocol Version 4, Src: 192.168.100.50, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 52262, Dst Port: 53
v Domain Name System (query)
  > Transaction ID: 0x5099
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > 1.debian.pool.ntp.org: type AAAA, class IN
```

```
0000  74 d2 1d 87 50 f1 00 0c  29 45 2d 24 08 00 45 00   t···P··· )E-$··E·
0010  00 43 be de 40 00 40 11  46 e1 c0 a8 64 32 08 08   ·C··@·@· F···d2··
0020  08 08 cc 26 00 35 00 2f  7d c1 50 99 01 00 00 01   ···&·5·/ }·P·····
0030  00 00 00 00 00 00 01 31  06 64 65 62 69 61 6e 04   ·******1 ·debian·
0040  70 6f 6f 6c 03 6e 74 70  03 6f 72 67 00 00 1c 00   pool·ntp ·org····
0050  01                                                 ·
```

- پیدا کردن سیستم‌های پر ترافیک DNS
- به منو :

- Statistics → Endpoints




Edit View Go Capture Analyze Statistics Telephony Wireless Help
dns
Time
Wireshark · Endpoints · Ethernet1
Endpoint Settings
Name resolution
Limit to display filter
Copy
Map
Protocol
Bluetooth
BPv7
DCCP
Ethernet
FC
FDDI
IEEE 802.11
Filter list for specific type
Ethernet · 2
IPv4 · 2
IPv6
TCP
UDP · 453
Address Packets Bytes Total Packets Percent Filtered Tx Packets Tx Bytes Rx
8.8.8.8 1,811 147 kB 1,811 100.00% 0 0 bytes
192.168.100.50 1,811 147 kB 5,889 30.75% 1,811 147 kB
Close
Help

- دنبال IP هایی باشید که:
- تعداد Query زیاد دارند
- درخواست‌های پشت سر هم می‌فرستند

- مثال:

- 192.168.1.45 → 500 DNS queries
- 192.168.1.12 → 15 DNS queries

- سیستم اول مشکوک‌تر است.

- **پیدا کردن دامنه‌های غیرعادی در DNS Traffic**
- هدف این است که از بین هزاران DNS Query، دامنه‌هایی را پیدا کنیم که **احتمالاً توسط Malware یا DNS Tunneling تولید شده‌اند.**

- **فیلتر کردن فقط DNS Query**
- ابتدا فقط درخواست‌های DNS را ببینید (نه پاسخ‌ها).
- dns.flags.response == 0

- **تحلیل:**
  - response == 0 یعنی
  - Queryresponse == 1 یعنی Response اکنون فقط درخواست‌هایی که سیستم‌ها برای Resolve کردن دامنه می‌فرستند نمایش داده می‌شوند.

Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.flags.response == 0

No.	Time	Source	Destination	Protocol	Length	Info
11…	5071.336182	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x024e AAAA 2.debian.pool.ntp.org
11…	5076.338897	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xfc75 A 2.debian.pool.ntp.org
11…	5076.338988	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x024e AAAA 2.debian.pool.ntp.org
11…	5081.343999	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xe128 A 3.debian.pool.ntp.org
11…	5081.344093	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x3925 AAAA 3.debian.pool.ntp.org
11…	5086.349771	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xe128 A 3.debian.pool.ntp.org
11…	5086.349918	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x3925 AAAA 3.debian.pool.ntp.org
11…	5091.355918	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x2e1f A 0.debian.pool.ntp.org
11…	5091.355918	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xd51d AAAA 0.debian.pool.ntp.org
11…	5096.361160	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x2e1f A 0.debian.pool.ntp.org
11…	5096.361390	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xd51d AAAA 0.debian.pool.ntp.org

```
> Frame 457: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \De
> Ethernet II, Src: VMware_45:2d:24 (00:0c:29:45:2d:24), Dst: HuaweiTechno_87:50:f1 (74
> Internet Protocol Version 4, Src: 192.168.100.50, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 52262, Dst Port: 53
v Domain Name System (query)
  > Transaction ID: 0x5099
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
```

```
0000  74 d2 1d 87 50 f1 00 0c  29 45 2d 24 08 00 45 00   t···P··· )E-$··E·
0010  00 43 be de 40 00 40 11  46 e1 c0 a8 64 32 08 08   ·C··@·@· F···d2··
0020  08 08 cc 26 00 35 00 2f  7d c1 50 99 01 00 00 01   ···&·5·/ }·P·····
0030  00 00 00 00 00 00 01 31  06 64 65 62 69 61 6e 04   ·····1 ·debian·
0040  70 6f 6f 6c 03 6e 74 70  03 6f 72 67 00 00 1c 00   pool·ntp ·org····
0050  01                                                 ·
```

- **نمایش نام دامنه‌ها**
- در Packet یکی از DNS Query ها را باز کنید.
- **فیلد مهم:**

- **dns.qry.name**

- **این همان نام دامنه‌ای است که سیستم درخواست کرده.**

Wireshark · Packet 11401 · Ethernet1

```
> Transaction ID: 0x9d97
> Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
v Queries
  > 3.debian.pool.ntp.org: type A, class IN

0000  74 d2 1d 87 50 f1 00 0c  29 45 2d 24 08 00 45 00   t···P··· )E-$··E·
0010  00 43 50 96 40 00 40 11  b5 29 c0 a8 64 32 08 08   ·CP·@·@· ·)··d2··
0020  08 08 9e b9 00 35 00 2f  79 2e 9d 97 01 00 00 01   ·····5·/ y.******
0030  00 00 00 00 00 00 01 33  06 64 65 62 69 61 6e 04   *******3 ·debian·
0040  70 6f 6f 6c 03 6e 74 70  03 6f 72 67 00 00 01 00   pool·ntp ·org····
0050  01                                                 ·
```

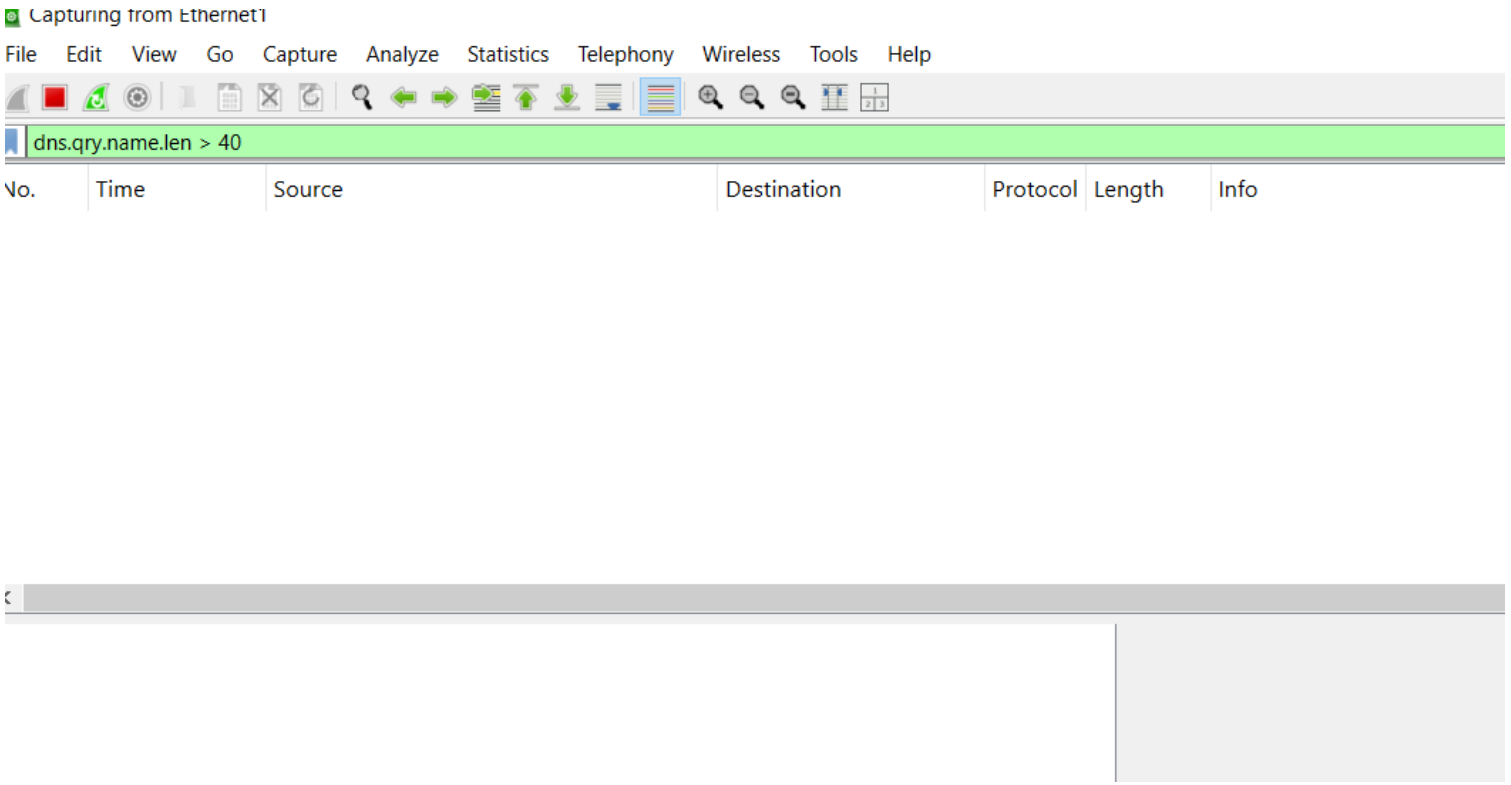
- **پیدا کردن دامنه‌های طولانی**
- بدافزارها و **DNS Tunneling** معمولاً **Subdomain** های بسیار طولانی تولید می‌کنند.
- **حالت طبیعی:**

- **google.com**
- **microsoft.com**
- **example.org**

- **حالت مشکوک:**

- a8sd7as9d8as7d9as8d7as9d.example.com
- d82kdn29d8d92kd92kdn92kd.domain.net

- در Wireshark می‌توان فیلتر طولانی بودن را بررسی کرد.
- dns.qry.name.len > 40
- تحلیل:
- دامنه‌هایی که طول آن‌ها بیشتر از ۴۰ کاراکتر است نمایش داده می‌شوند.



تمرکز روی Subdomainهای طولانی

- DNS Tunnelingمعمولاً در Subdomainاتفاق می‌افتد، نه کل دامنه.
- **مثال مشکوک:**
- **as8d7a9sd8a7sd98a7sd9a87sd.domain.com**
- می‌توانید تمرکز را روی رشته‌های طولانی قبل از دامنه اصلی بگذارید.
- **فیلتر وایرشارک**

- **dns.qry.name contains "."**

Capturing from Ethernet1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.qry.name contains "."

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x29b1 A 3.debian.pool.ntp.org
2	0.000000	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x19ba AAAA 3.debian.pool.ntp.org
12	5.007040	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xac3b A 0.debian.pool.ntp.org
13	5.007040	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x3422 AAAA 0.debian.pool.ntp.org
25	10.013153	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xac3b A 0.debian.pool.ntp.org
26	10.013153	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x3422 AAAA 0.debian.pool.ntp.org
34	15.019448	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xd8db A 1.debian.pool.ntp.org
35	15.020423	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xe7c5 AAAA 1.debian.pool.ntp.org
42	20.025337	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xd8db A 1.debian.pool.ntp.org
43	20.025452	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xe7c5 AAAA 1.debian.pool.ntp.org
50	25.041821	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xf13d A 2.debian.pool.ntp.org
51	25.041821	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x6237 AAAA 2.debian.pool.ntp.org

```
> Frame 1: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Devi
> Ethernet II, Src: VMware_45:2d:24 (00:0c:29:45:2d:24), Dst: HuaweiTechno_87:50:f1 (74
> Internet Protocol Version 4, Src: 192.168.100.50, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 42539, Dst Port: 53
v Domain Name System (query)
  > Transaction ID: 0x29b1
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
```

```
0000  74 d2 1d 87 50 f1 00 0c  29 45 2d 24 08 00 45 00   t···P··· )E-$··E·
0010  00 43 a1 03 40 00 40 11  64 bc c0 a8 64 32 08 08   ·C··@·@· d···d2··
0020  08 08 a6 2b 00 35 00 2f  e5 a2 29 b1 01 00 00 01   ···+·5·/ ··)·····
0030  00 00 00 00 00 00 01 33  06 64 65 62 69 61 6e 04   ·******3 ·debian·
0040  70 6f 6f 6c 03 6e 74 70  03 6f 72 67 00 00 01 00   pool·ntp ·org····
0050  01                                                 ·
```

• فیلتر

•dns && dns.flags.response == 0

Capturing from Ethernet1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns && dns.flags.response == 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x29b1 A 3.debian.pool.ntp.org
2	0.000000	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x19ba AAAA 3.debian.pool.ntp.org
12	5.007040	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xac3b A 0.debian.pool.ntp.org
13	5.007040	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x3422 AAAA 0.debian.pool.ntp.org
25	10.013153	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xac3b A 0.debian.pool.ntp.org
26	10.013153	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x3422 AAAA 0.debian.pool.ntp.org
34	15.019448	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xd8db A 1.debian.pool.ntp.org
35	15.020423	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xe7c5 AAAA 1.debian.pool.ntp.org
42	20.025337	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xd8db A 1.debian.pool.ntp.org
43	20.025452	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xe7c5 AAAA 1.debian.pool.ntp.org
50	25.041821	192.168.100.50	8.8.8.8	DNS	81	Standard query 0xf13d A 2.debian.pool.ntp.org
51	25.041821	192.168.100.50	8.8.8.8	DNS	81	Standard query 0x6237 AAAA 2.debian.pool.ntp.org

```
> Frame 26: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Dev
> Ethernet II, Src: VMware_45:2d:24 (00:0c:29:45:2d:24), Dst: HuaweiTechno_87:50:f1 (74
> Internet Protocol Version 4, Src: 192.168.100.50, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 42736, Dst Port: 53
v Domain Name System (query)
  > Transaction ID: 0x3422
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
```

```
0000  74 d2 1d 87 50 f1 00 0c  29 45 2d 24 08 00 45 00   t···P··· )E-$··E·
0010  00 43 9b 23 40 00 40 11  6a 9c c0 a8 64 32 08 08   ·C·#@·@· j···d2··
0020  08 08 a6 f0 00 35 00 2f  bf 6f 34 22 01 00 00 01   ·····5·/ ·o4"····
0030  00 00 00 00 00 00 01 30  06 64 65 62 69 61 6e 04   ·····0 ·debian·
0040  70 6f 6f 6c 03 6e 74 70  03 6f 72 67 00 00 1c 00   pool·ntp ·org····
0050  01                                                 ·
```

Capturing from Ethernet1

File Edit View Go Capture Analyze Statistics

dns && dns.flags.response == 0

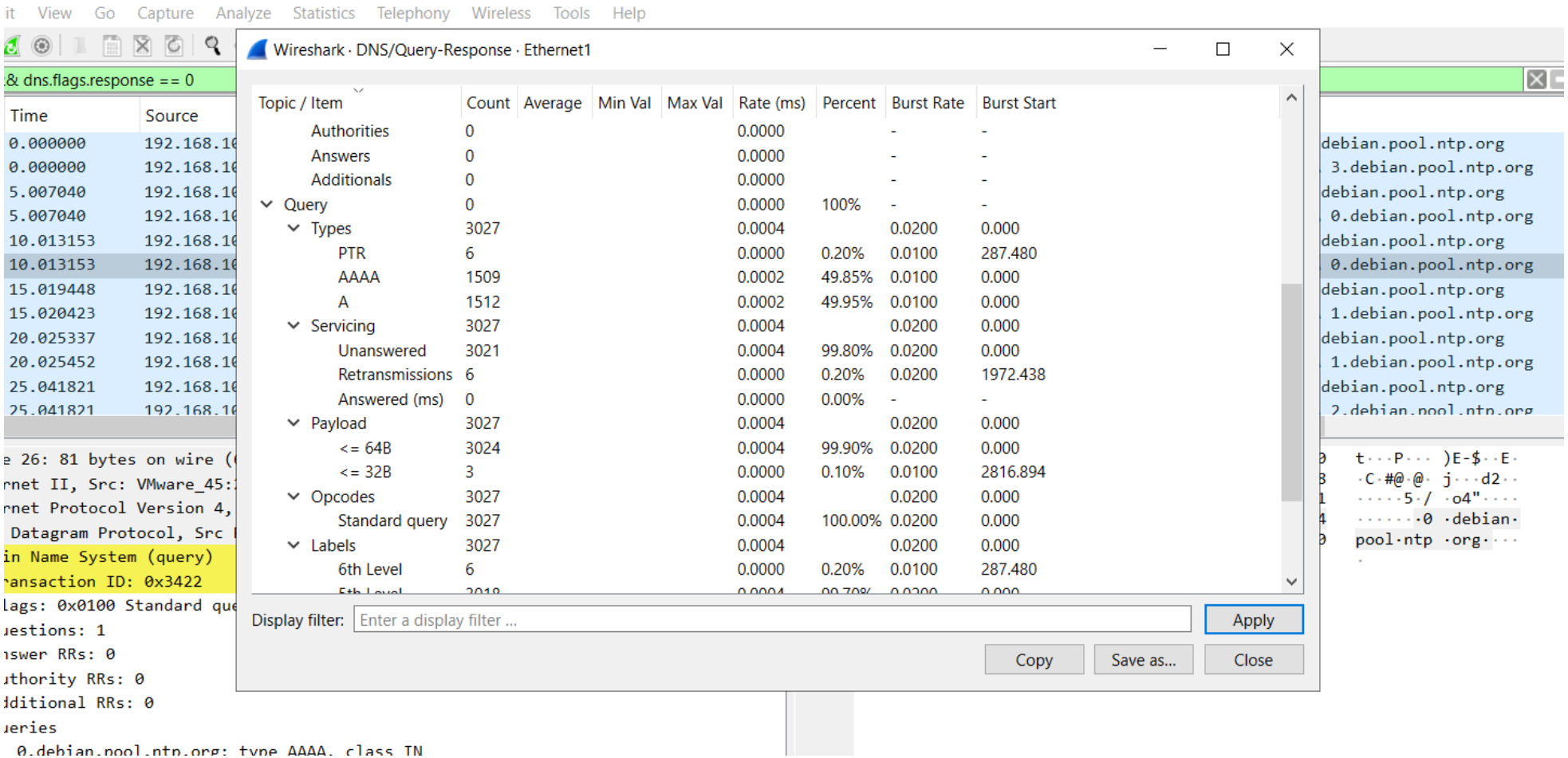
No.	Time	Source
1	0.000000	192.168.100.50
2	0.000000	192.168.100.50
12	5.007040	192.168.100.50
13	5.007040	192.168.100.50
25	10.013153	192.168.100.50
26	10.013153	192.168.100.50
34	15.019448	192.168.100.50
35	15.020423	192.168.100.50
42	20.025337	192.168.100.50
43	20.025452	192.168.100.50
50	25.041821	192.168.100.50
51	25.041821	192.168.100.50

```
> Frame 26: 81 bytes on wire (648 bits), 81
> Ethernet II, Src: VMware_45:2d:24 (00:0c:2
> Internet Protocol Version 4, Src: 192.168.
> User Datagram Protocol, Src Port: 42736, D
v Domain Name System (query)
  > Transaction ID: 0x3422
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > 0.debian.pool.ntp.org: type AAAA, cl
```

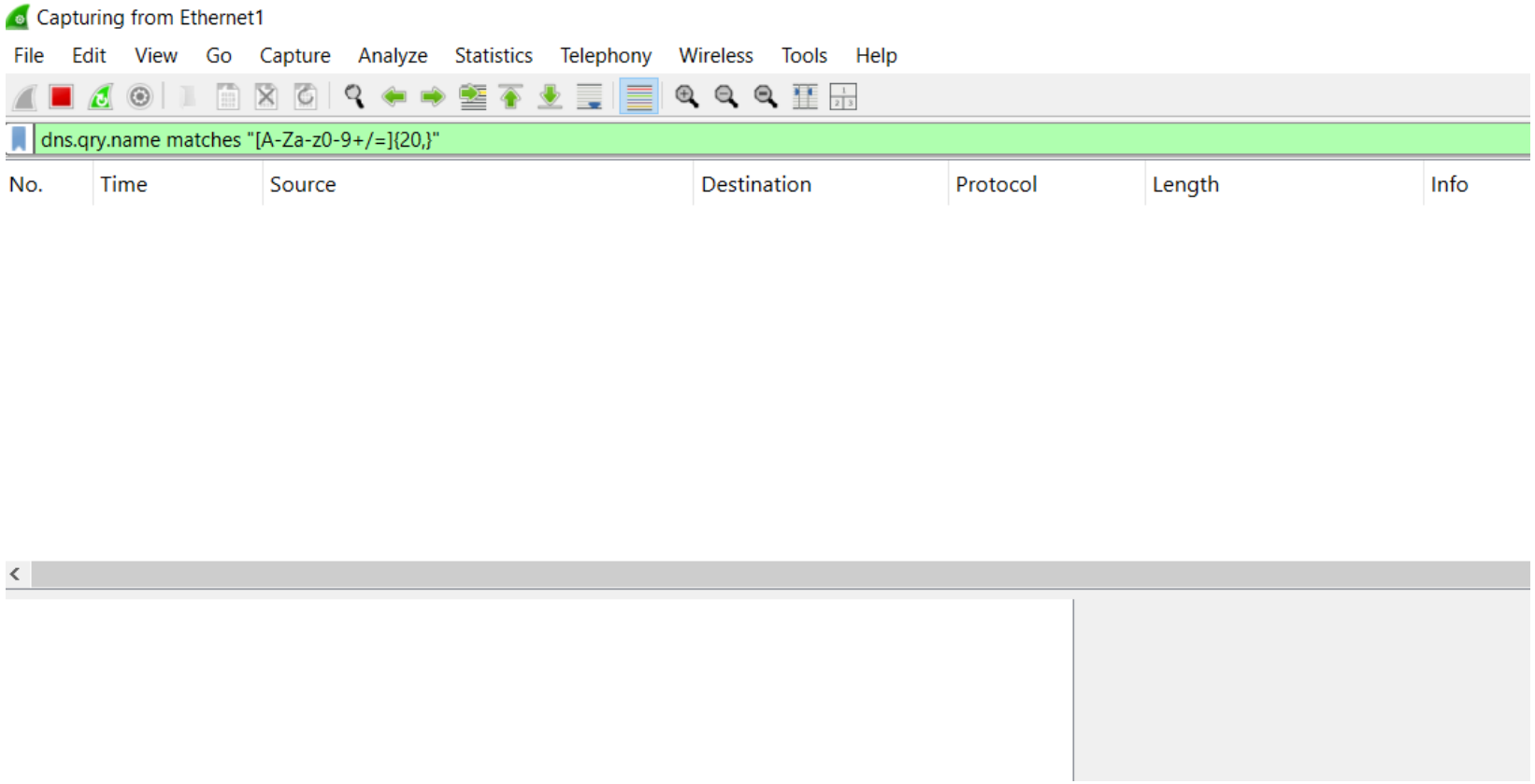
wireshark_Ethernet1V5OPP3.pcapng

Capture File Properties	Ctrl+Alt+Shift+C	IPv6 Statistics
Resolved Addresses		
Protocol Hierarchy		
Conversations		
Endpoints		
Packet Lengths		
I/O Graphs		
Service Response Time		
DHCP (BOOTP) Statistics		
NetPerfMeter Statistics		
ONC-RPC Programs		
29West		
ANCP		
BACnet		
Collectd		
DNS		
Flow Graph		
HART-IP		
HPFEEDS		
HTTP		
HTTP2		
Sametime		
TCP Stream Graphs		
UDP Multicast Streams		
Reliable Server Pooling (RSerPool)		
SOME/IP		
DTN		
F5		

- و دامنه‌هایی که:
- تعداد Query زیاد دارند
- نام نامفهوم دارند

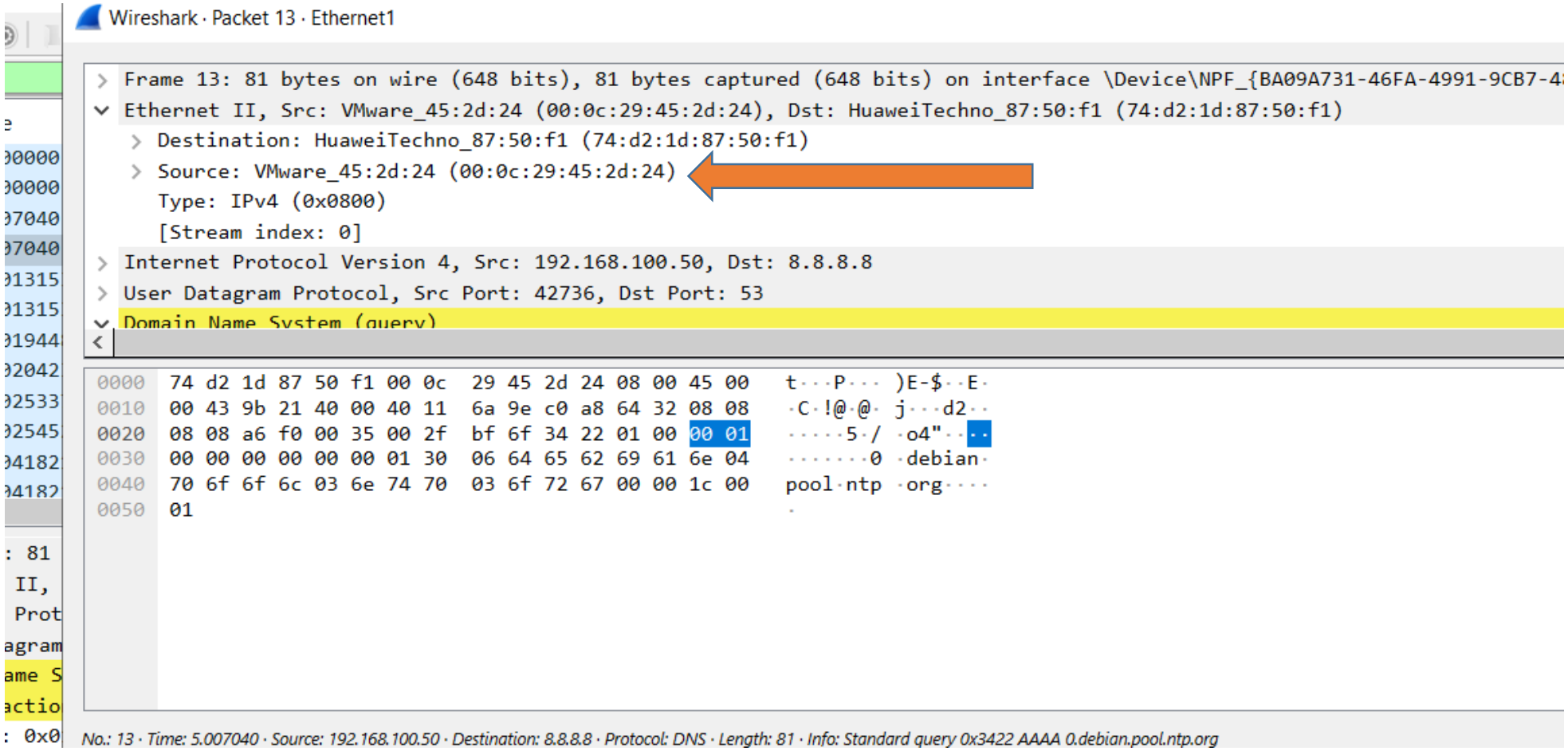


- خیلی از DNS Tunnelها از Base64استفاده می‌کنند.
- فیلتر جستجو :
- dns.qry.name matches "[A-Za-z0-9+/=]{20,}"
- اگر چنین دامنه‌هایی زیاد دیدید → احتمال Tunnelزیاد است.

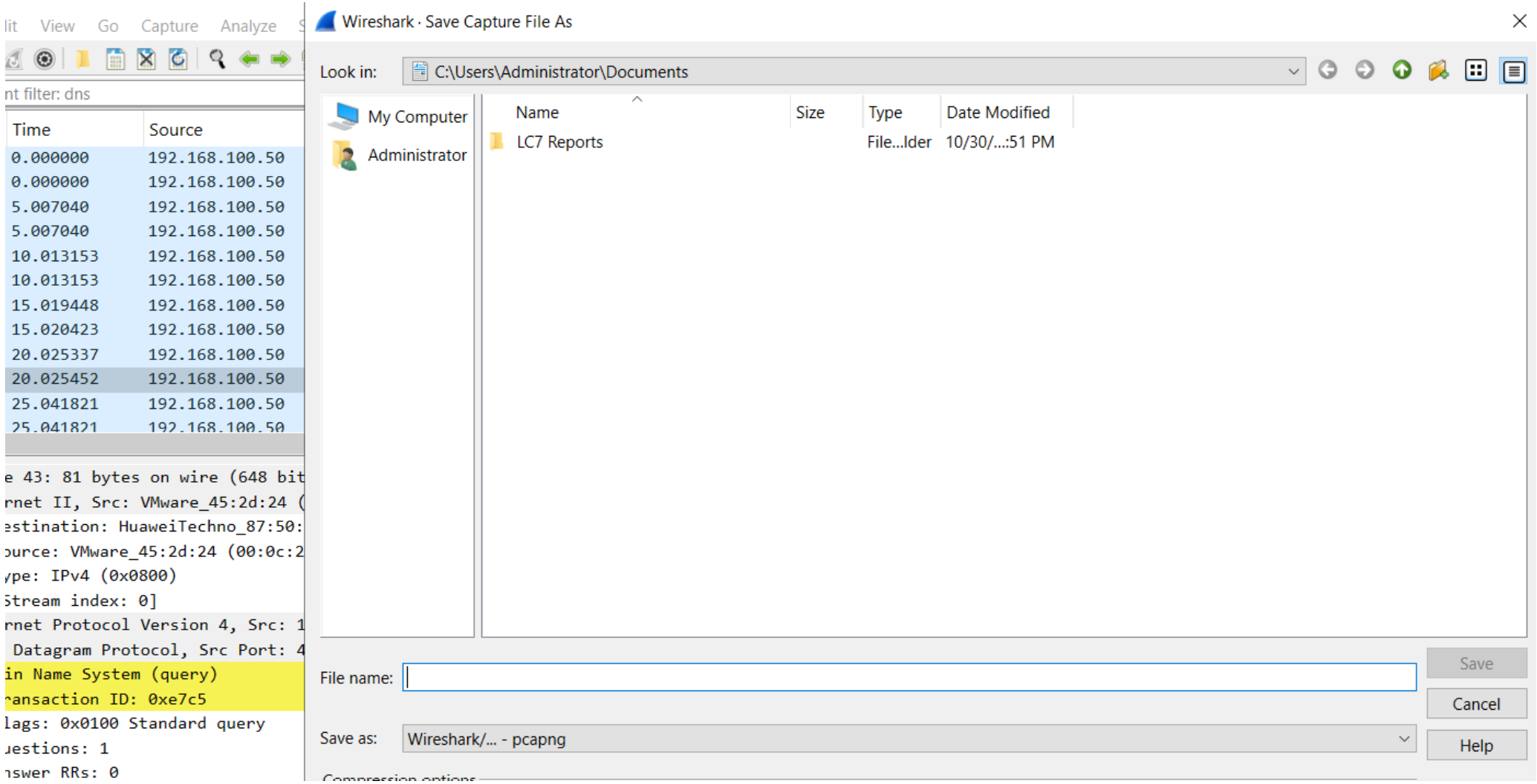


- وقتی دامنه مشکوک پیدا شد:
- روی Packet کلیک کنید و ببینید:

- Source IP



روش ۳۰ ثانیه‌ای پیدا کردن سیستم آلوده در فایل PCAP در پروژه های SOC



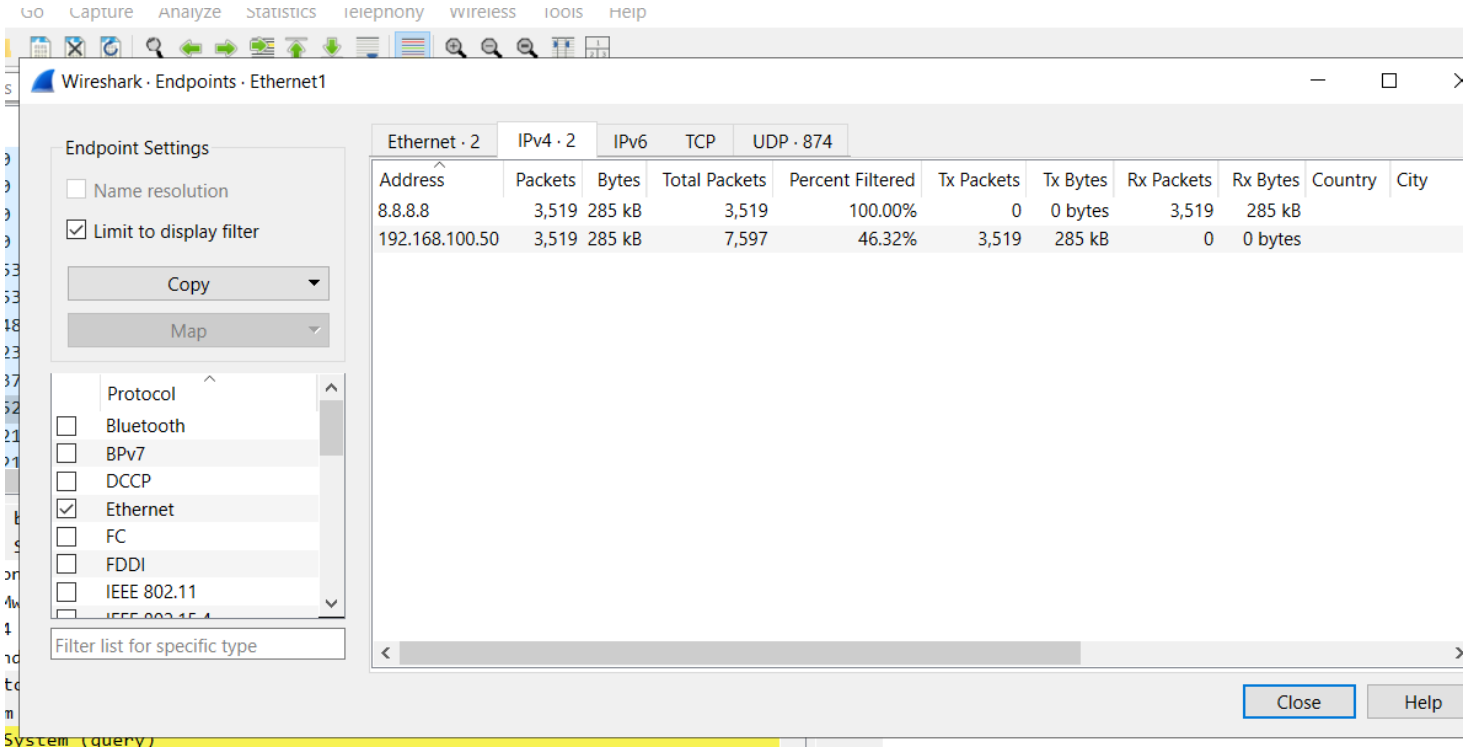
- در یک PCAP بزرگ مثلاً صدها هزار Packet اگر بخواهید مثل حالت عادی Packet-به- Packet جلو بروید، زمان زیادی می‌برد. در پروژه های SOC معمولاً از یک روش تحلیلی سریع Top-Down استفاده می‌کنند تا در کمتر از ۳۰ ثانیه سیستم مشکوک را پیدا کنند.

- به جای بررسی Packet ها، ابتدا **آمار کلی ترافیک** را بررسی می‌کنیم تا Host غیرعادی را پیدا کنیم.
- ترتیب مراحل:
- Statistics → Identify abnormal host → Investigate traffic

- باز کردن فایل PCAP
- اجازه بدهید Wiresharkفایل را Indexکند.
- پیدا کردن سیستم‌های فعال

- Statistics → Endpoints
- IPv4

- در اینجا لیست تمام IPها نمایش داده می‌شود.



- ستون‌های مهم:

- Packets
- Bytes
- Tx
- Rx

- چه چیزی مشکوک است؟

- 192.168.1.10 200 packets
- 192.168.1.15 180 packets
- 192.168.1.22 120 packets
- 192.168.1.45 **9500** packets

- IPمشکوک
- ip.addr == 192.168.1.45
- اکنون فقط ترافیک همان Hostرا می‌بینید.
- به ستون Destinationنگاه کنید.
- 192.168.1.45 → **8.8.8.8**
- 192.168.1.45 → 142.250.190.14
- 192.168.1.45 → 185.231.67.21
- اگر یک IPخارجی زیاد تکرار شود:
- 185.231.67.21

- اکنون ببینید این سیستم چه دامنه‌هایی Resolve کرده است.
- dns && ip.addr == 192.168.1.45
- به دنبال دامنه‌های مشکوک باشید

- بررسی Port Scan
- tcp.flags.syn == 1 && tcp.flags.ack == 0
- اگر این سیستم SYN زیادی بفرستد:
- Possible scanning or worm

Windows LAPS (Local Administrator Password Solution)

- نسخه جدید مایکروسافت برای مدیریت امن پسورد اکانت‌های **Local Administrator** روی سیستم‌های ویندوزی است.
- این قابلیت از Windows 11 / Windows Server 2022 به بعد **به‌صورت Built-in در ویندوز وجود دارد** و جایگزین LAPS قدیمی شده است.

- هدف اصلی آن این است که **پسورد Administrator روی همه سیستم‌ها یکسان نباشد** و به‌صورت **اتوماتیک، تصادفی و دوره‌ای تغییر کند.**

- **مشکل امنیتی که LAPS حل می‌کند**
- در بسیاری از شبکه‌ها:
- روی همه Workstationها یک Local Admin وجود دارد
- پسورد آن روی همه سیستم‌ها یکسان است

- **مثلاً:**

- Administrator : P@ssword123

- اگر مهاجم فقط **یک سیستم را compromise کند** می‌تواند با همان پسورد:
- به بقیه سیستم‌ها login کند
- lateral movement انجام دهد
- credential harvesting کند
- این دقیقاً همان حمله‌ای است که در BloodHound زیاد دیده می‌شود.

- **کاری که Windows LAPS انجام می‌دهد**
- برای هر کامپیوتر:
- یک **پسورد تصادفی و قوی** تولید می‌کند
- آن را در **Active Directory** یا **Azure AD** ذخیره می‌کند
- پسورد را **به‌صورت دوره‌ای تغییر می‌دهد**

- مثال:

- **PC-1** → kF#92!ds@aQ1
- **PC-2** → Wq!3sa$Xz19
- **PC-3** → R!d$29AlaP@

مثال سازمانی و اجرایی

- **فرض کنید** در یک شرکت **۲۰۰** کامپیوتر داریم.
- **روی همه آن‌ها یک اکانت** Local Administrator وجود دارد.
- و روی همه آن‌ها یک پسورد یکسان تنظیم شده:

- Administrator : Company@123

- **اتفاق خطرناک این است که:**
- اگر مهاجم فقط **یکی** از این سیستم‌ها را هک کند
- پسورد ادمین محلی را به دست بیاورد
- می‌تواند با همان پسورد برود سراغ بقیه سیستم‌ها
- یعنی از یک سیستم آلوده، به سیستم‌های دیگر هم حرکت کند.

- به این می‌گویند:
- **Lateral Movement**
- حرکت جانبی مهاجم در شبکه

LAPS آمده دقیقاً این مشکل را حل کند

LAPS می‌گوید:

پسورد Administrator محلی هر سیستم باید با بقیه فرق داشته باشد، قوی باشد، و هر چند وقت یک‌بار خودکار عوض شود.

چرا اصلاً Local Administrator وجود دارد؟

اکانت **Local Administrator** یک حساب مدیریتی داخلی روی هر سیستم است که مستقل از Domain کار می‌کند. یعنی حتی اگر:

- سیستم به Domain وصل نباشد
- ارتباط با Domain Controller قطع شود
- مشکل در احراز هویت دامنه پیش بیاید

باز هم می‌توان با این حساب **مدیریت سیستم را انجام داد.**

به همین دلیل حذف کامل آن معمولاً توصیه نمی‌شود.

- **خب یک سوال** User local Administrator که به تور پیش فرض در سیستم کلاینت ها غیرفعال هست باز هم کاربرد دارد ؟

- بله، **هنوز هم کاربرد دارد**؛ حتی اگر در ویندوزهای جدید به‌صورت پیش‌فرض **غیرفعال Disabled** باشد. اما نحوه استفاده از آن در محیط‌های سازمانی کمی متفاوت و کنترل‌شده است.

- **چرا در ویندوزهای جدید غیرفعال است؟**
- مایکروسافت آن را پیش‌فرض غیرفعال گذاشته چون در گذشته:
- بسیاری از سازمان‌ها یک **پسورد یکسان** روی همه سیستم‌ها می‌گذاشتند
- مهاجم اگر آن پسورد را پیدا می‌کرد می‌توانست به همه سیستم‌ها دسترسی بگیرد
- پس برای کاهش ریسک، اکانت به‌صورت پیش‌فرض **Disabled** است.

در عمل در سازمان‌ها چگونه استفاده می‌شود؟

- **سه مدل رایج وجود دارد.**
- **۱. فعال اما مدیریت‌شده با LAPS (مدل توصیه‌شده)**
- در بیشتر سازمان‌ها:
- Local Administrator **فعال می‌شود**
- ولی پسورد آن با **Windows LAPS** مدیریت می‌شود
- **ویژگی‌ها:**
- پسورد برای هر سیستم متفاوت است
- پسورد مرتب عوض می‌شود
- در AD ذخیره می‌شود
- فقط Helpdesk یا Adminها می‌توانند آن را ببینند
- این **مدل استاندارد Hardening** برای Workstationها است.

غیرفعال نگه داشتن کامل

- **برخی سازمان‌ها:**
- Local Administrator را **کاملاً غیرفعال** می‌کنند
- فقط از **Domain Admin / Endpoint Management** استفاده می‌کنند
- مشکل این مدل:
- اگر سیستم از Domain جدا شود
- یا ارتباط با DC قطع شود
- مدیریت سیستم سخت می‌شود.

بهترین Practice در Hardening

- در اکثر پروژه‌های امنیتی پیشنهاد این است:

1. اکانت Local Administrator **فعال باشد**
2. نام آن **rename شود**
3. پسورد آن توسط **Windows LAPS** مدیریت شود
4. دسترسی خواندن پسورد محدود باشد
5. از آن فقط برای **Emergency / Break-Glass** استفاده شود

- **Local Administrator**مثل یک «کلید اضطراری» برای هر کامپیوتر است.
- معمولاً از آن استفاده روزمره نمی‌کنیم، اما اگر مشکلی در شبکه یا Domainپیش بیاید، می‌توانیم با آن وارد سیستم شویم.
- برای اینکه این کلید خطرناک نشود، از **Windows LAPS**استفاده می‌کنیم تا پسورد آن برای هر سیستم متفاوت و مرتب تغییر کند.

- **تفاوت بین این سه مورد در ویندوز:**

- Local Administrator
- Domain Admin
- Local Admin (گروهAdministrators)

- **Local Administrator**
- **Local Administrator** یک **اکانت محلی** است که فقط روی همان کامپیوتر وجود دارد.

- ویژگی‌ها:
- در **SAM دیتابیس همان سیستم** ذخیره می‌شود
- فقط روی **همان کامپیوتر** دسترسی کامل دارد
- به Domain وابسته نیست
- اگر شبکه یا Domain قطع شود هنوز قابل استفاده است

- **Domain Admin**
  - **Domain Admin** یک **اکانت دامینی** است که در **Active Directory** تعریف شده است

- ویژگی‌ها:
- در **Active Directory** ذخیره می‌شود
- روی **کل Domain** قدرت مدیریتی دارد
- می‌تواند:
  - Domain Controller را مدیریت کند
  - یوزر بسازد
  - GPO تغییر دهد
  - روی همه سیستم‌ها Admin شود
- نکته مهم:
- اعضای گروه **Domain Admins** به‌صورت پیش‌فرض عضو گروه **Administrators همه سیستم‌های Domain** هستند

- **این یکی یک گروه است، نه یک اکانت.**
- این گروه روی هر کامپیوتر وجود دارد.
- اعضای این گروه می‌توانند:
- سیستم را کامل مدیریت کنند
- نرم‌افزار نصب کنند
- سرویس‌ها را تغییر دهند
- اما اعضای آن می‌توانند انواع مختلفی باشند.
- مثلاً داخل گروه Administrators ممکن است این‌ها باشند:

- **یعنی:**
- یک اکانت محلی
- یک گروه دامینی
- یک کاربر دامینی
- همه می‌توانند **Local Admin آن سیستم شوند.**

- در شبکه‌های ویندوزی معمولاً روی همه کامپیوترها یک اکانت Administratorمحلی وجود دارد.
- اگر پسورد این اکانت روی همه سیستم‌ها یکی باشد، مهاجم با به‌دست آوردن آن از یک سیستم می‌تواند به بقیه سیستم‌ها هم نفوذ کند.
- Windows LAPSاین مشکل را حل می‌کند.

- این قابلیت برای هر کامپیوتر یک پسورد متفاوت، قوی و زمان‌دار تولید می‌کند و آن را در Active Directoryذخیره می‌کند تا فقط ادمین‌های مجاز بتوانند آن را ببینند.

- به این ترتیب، اگر یک سیستم آلوده شود، مهاجم نمی‌تواند با همان پسورد به همه سیستم‌های دیگر حرکت کند

اجراي خودكار Autoplay براي دستگاه هاي volume-non بايد خاموش (غير فعال) باشد

- اجرا خودكار ممكن است اجازه دهد كه كد هاي مخرب بر روي سيستم اجرا شود . از آنجا كه پخش خودكار باعث ميشود به محض قرار گرفتن يک ورودي در دستگاه مانند نتايج يک برنامه، فايلهاي تنظيمی يا موزيک و ... آن ها خوانده شود پس اين تنظيمات بايد براي دستگاه هاي volume-non مانند devices MTP غير فعال باشد چون ممكن است باعث اجراي يک سري كد مخرب در سيستم شود.

- به مسير زير رفته و مقدار devices volume-non for Autoplay Disallow را Enabled تغيير ميدهيم:

- Configure the policy value for Computer Configuration -> Administrative Templates -> Windows
- Components -> AutoPlay Policies

s [WIN-0HUUI5I7G1D.KIYAN.NET] Policy
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates: Policy definiti
      - Control Panel
      - Network
      - Printers
      - Server
      - Start Menu and Taskbar
      - System
      - Windows Components
        - ActiveX Installer Service
        - Add features to Windows 10
        - App Package Deployment
        - App Privacy
        - App runtime
        - Application Compatibility
        - AutoPlay Policies
        - Biometrics
        - BitLocker Drive Encryption
        - Camera

Administrative Templates: Policy definitions (ADMX files) retrieved from the l

Select an item to view its description.

Setting
- Control Panel
- Network
- Printers
- Server
- Start Menu and Taskbar
- System
- Windows Components
- All Settings

Group Policy Management Editor

File Action View Help

s [WIN-0HUUI5I7G1D.KIYAN.NET] Policy
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
    - Administrative Templates: Policy definiti
      - Control Panel
      - Network
      - Printers
      - Server
      - Start Menu and Taskbar
      - System
      - Windows Components
        - ActiveX Installer Service
        - Add features to Windows 10
        - App Package Deployment
        - App Privacy
        - App runtime
        - Application Compatibility
        - AutoPlay Policies
        - Biometrics
        - BitLocker Drive Encryption
        - Camera
        - Cloud Content

AutoPlay Policies

Select an item to view its description.

Setting
- Turn off Autoplay
- Prevent AutoPlay from remembering user choices.
- Disallow Autoplay for non-volume devices
- Set the default behavior for AutoRun

اجراي خودكار Autoplay بايد بر روي درايورها غير فعال باشند

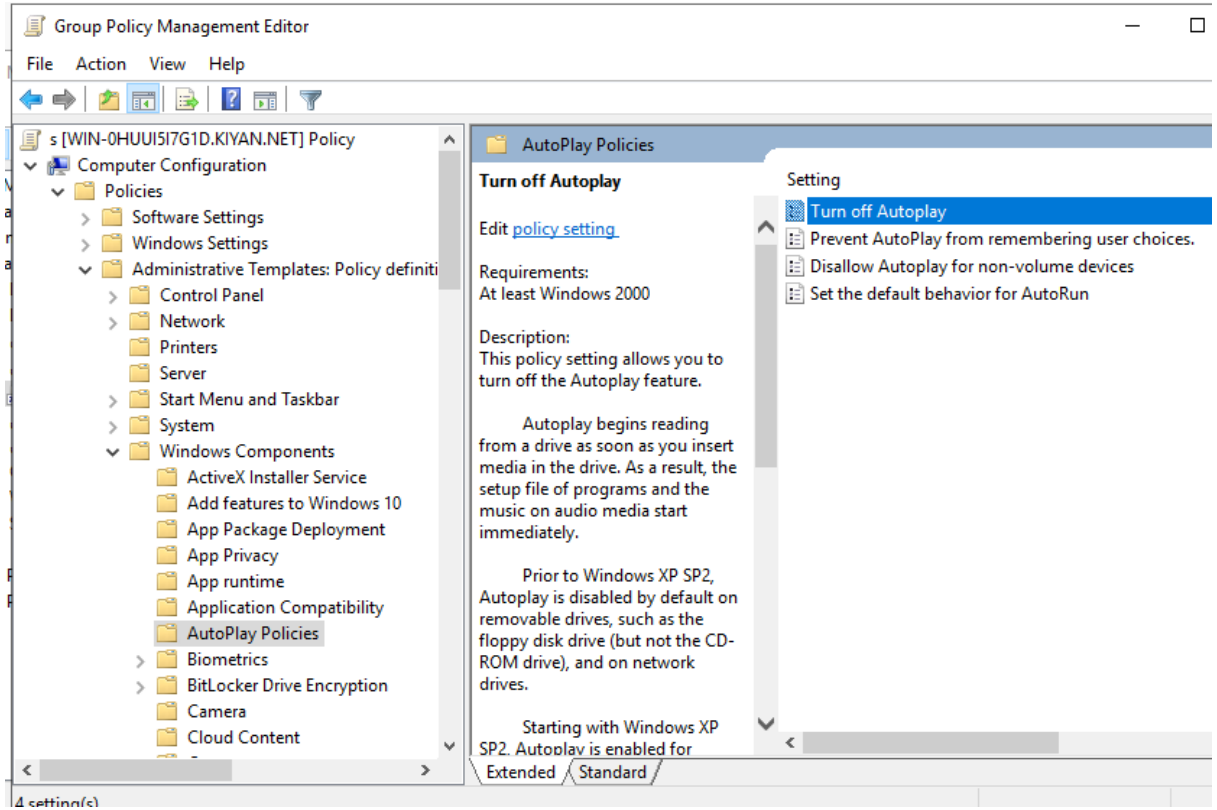
- اجرا خودکار ممکن است اجازه دهد که کد های مخرب بر روی سیستم اجرا شود .

- از آنجا که پخش خودکار باعث میشود به محض قرار گرفتن یک ورودی در دستگاه مانند نتایج یک برنامه، فایلهای تنظیمی یا موزیک و ... آن ها خوانده شود و بطور پیشفرض اجرای خودکار برروی درایورهای قابل پاک شدن مانند فلاپی CD-Rom غیر فعال است

- پس این تنظیمات باید بر روی همه درایورها غیر فعال باشد چون ممکن است باعث اجرای یک سری کد مخرب در سیستم شود.

- به مسیر زیر رفته و مقدار "Turn off AutoPlay" را به "All Drives:Enabled" تغییر میدهیم:

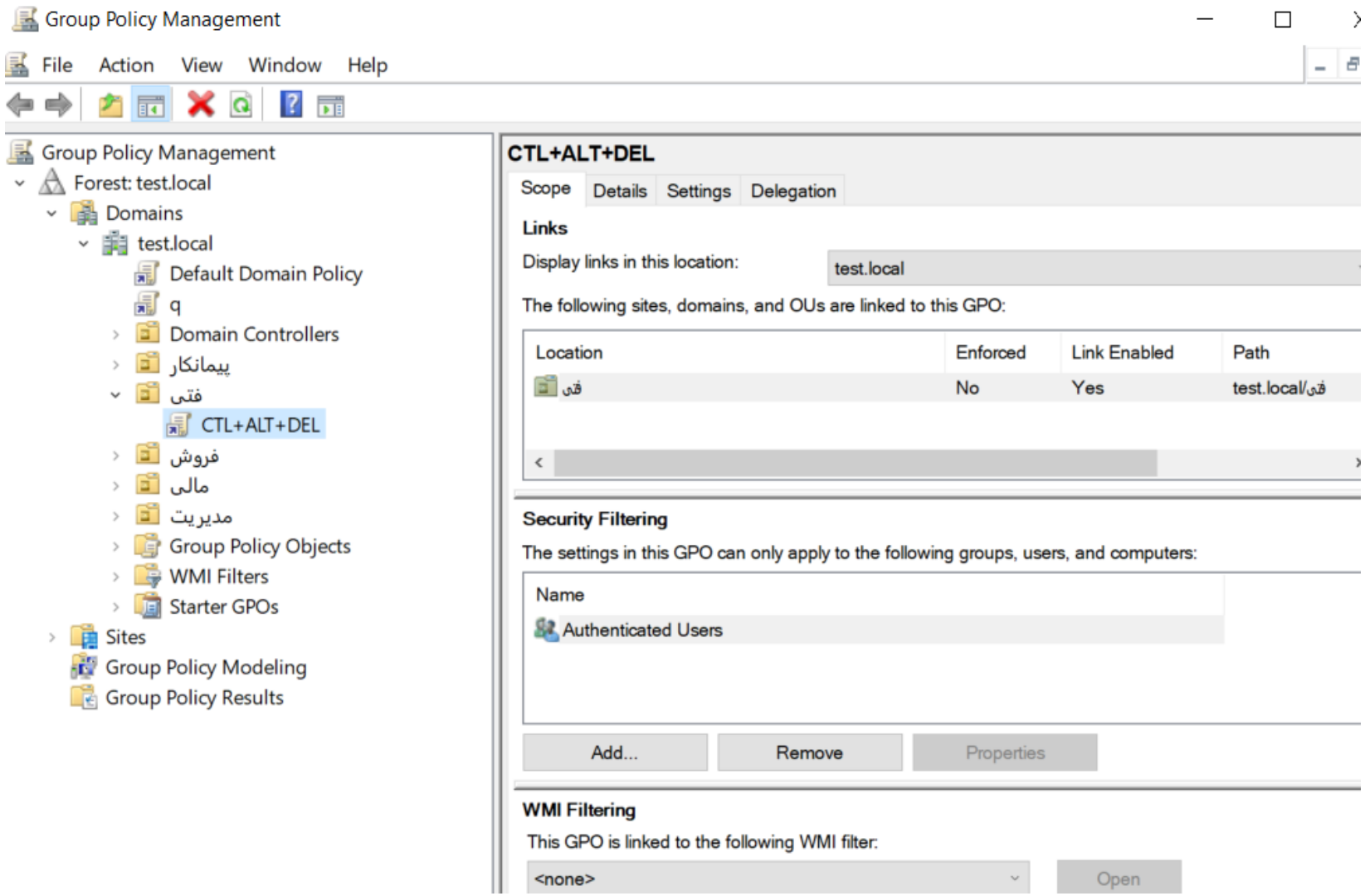
- Configure the policy value for Computer Configuration -> Administrative Templates -> Windows
- Components -> AutoPlay Policies



پیاده‌سازی Privileged Access Workstation (PAW)

- PAW یعنی یک سیستم جداگانه فقط برای مدیریت
- یک کامپیوتر جدا در شبکه مدیریتی بساز
- عضو Domain نمایید
- فقط ادمین‌ها اجازه لاگین داشته باشند.

- Computer Configuration
- Windows Settings
- Security Settings
- Local Polices
- User Rights Assignment
- Allow log on locally



Group Policy Management Editor

File Action View Help

- Default Domain Policy [SERVER1.TEST.LOCAL] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Deployed Printers
        - Security Settings
          - Account Policies
          - Local Policies
            - Audit Policy
            - User Rights Assignment
            - Security Options
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Policies
          - Windows Defender Firewall with Advanced Se
          - Network List Manager Policies
          - Wireless Network (IEEE 802.11) Policies
          - Public Key Policies

Policy	Policy
Access Credential Manager as a trusted caller	Not D
Access this computer from the network	Not D
Act as part of the operating system	Not D
Add workstations to domain	Not D
Adjust memory quotas for a process	Not D
Allow log on locally	Not D
Allow log on through Remote Desktop Services	Not D
Back up files and directories	Not D
Bypass traverse checking	Not D
Change the system time	Not D
Change the time zone	Not D
Create a pagefile	Not D
Create a token object	Not D
Create global objects	Not D
Create permanent shared objects	Not D
Create symbolic links	Not D
Debug programs	Not D
Deny access to this computer from the network	Not D
Deny log on as a batch job	Not D
Deny log on as a service	Not D
Deny log on locally	Not D
Deny log on through Remote Desktop Services	Not D

فعال کردن Audit Logging

- Group Policy Management
- Default Domain Controllers Policy
- Computer Configuration
- Policies
- Windows Settings
- Security Settings
- Advanced Audit Policy Configuration
- Audit Policies

Group Policy Management Editor

File Action View Help

- Restricted Groups
- System Services
- Registry
- File System
- Wired Network (IEEE 802.3) Policies
- Windows Defender Firewall with Advanced Se
- Network List Manager Policies
- Wireless Network (IEEE 802.11) Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Active Directory (TEST.L
- Advanced Audit Policy Configuration
  - Audit Policies
    - Account Logon
    - Account Management
    - Detailed Tracking
    - DS Access
    - Logon/Logoff
    - Object Access
    - Policy Change
    - Privilege Use
    - System
    - Global Object Access Auditing

Advanced

Getting Started

Advanced Audit Policy Configuration settings can be used to provide detailed c
policies, identify attempted or successful attacks on your network and resource
compliance with rules governing the management of critical organizational asse

When Advanced Audit Policy Configuration settings are used, the "Au
policy subcategory settings (Windows Vista or later) to override audit p
settings" policy setting under Local Policies\Security Options must also

More about

Which editions of

A summary

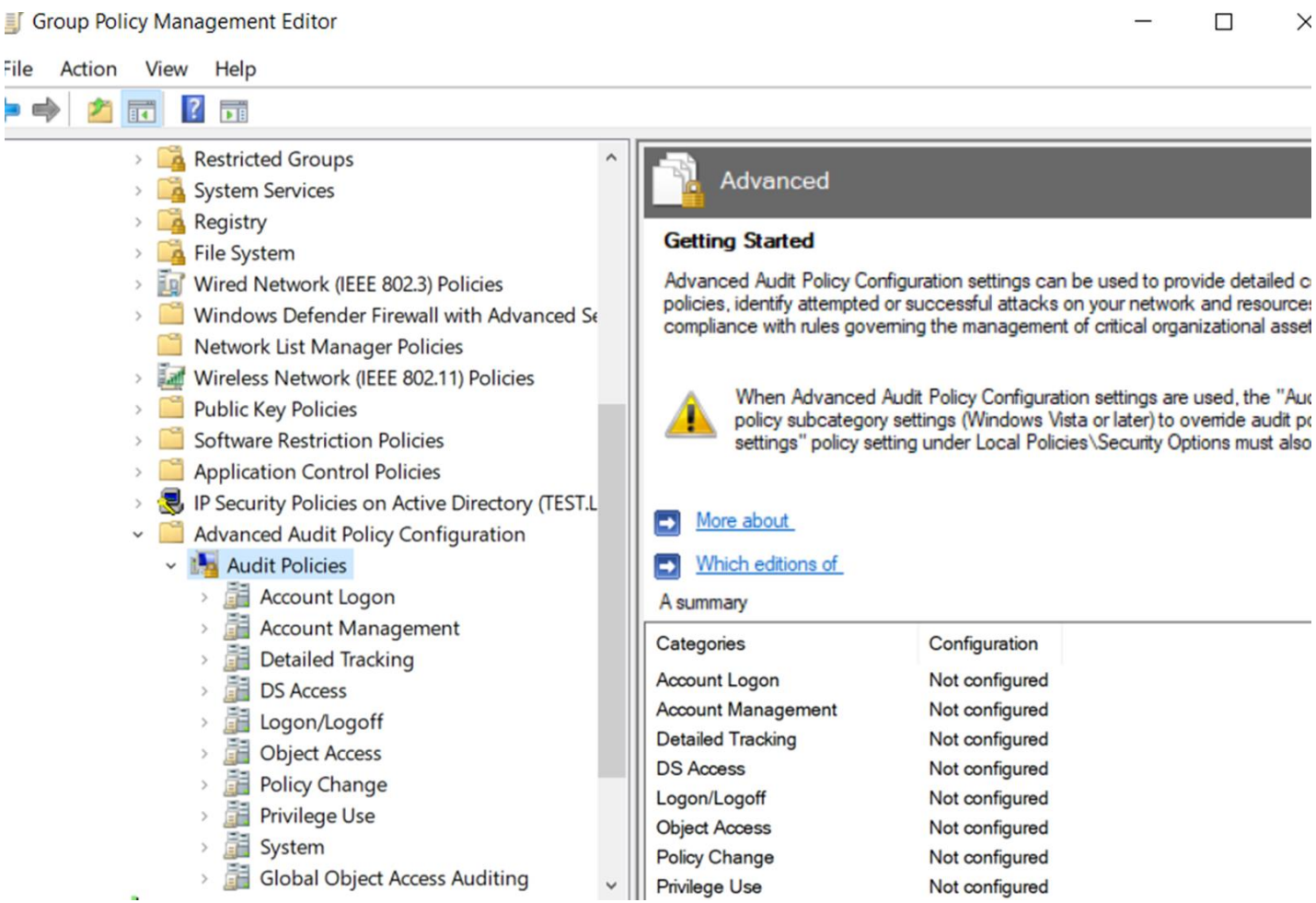
Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured

• فعال کن:

• همه را روی:

• Success and Failure

•Audit Logon
•Audit Account Logon
•Audit Directory Service Access
•Audit Policy Change
•Audit Privilege Use



مانیتور کردن Event Logs

- روی Domain Controller:
- Event Viewer
- مهم‌ترین لاگ‌ها:
- Security Log
- Directory Service Log
- System Log

Event Viewer

File Action View Help

- Event Viewer (Local)
  - Custom Views
  - Windows Logs
    - Application
    - Security
    - Setup
    - System
    - Forwarded Events
  - Applications and Services Log
  - Subscriptions

Event Viewer (Local)

Overview and Summary

Reading data, please wait...

Overview

To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the logs is shown below.

Summary of Administrative Events

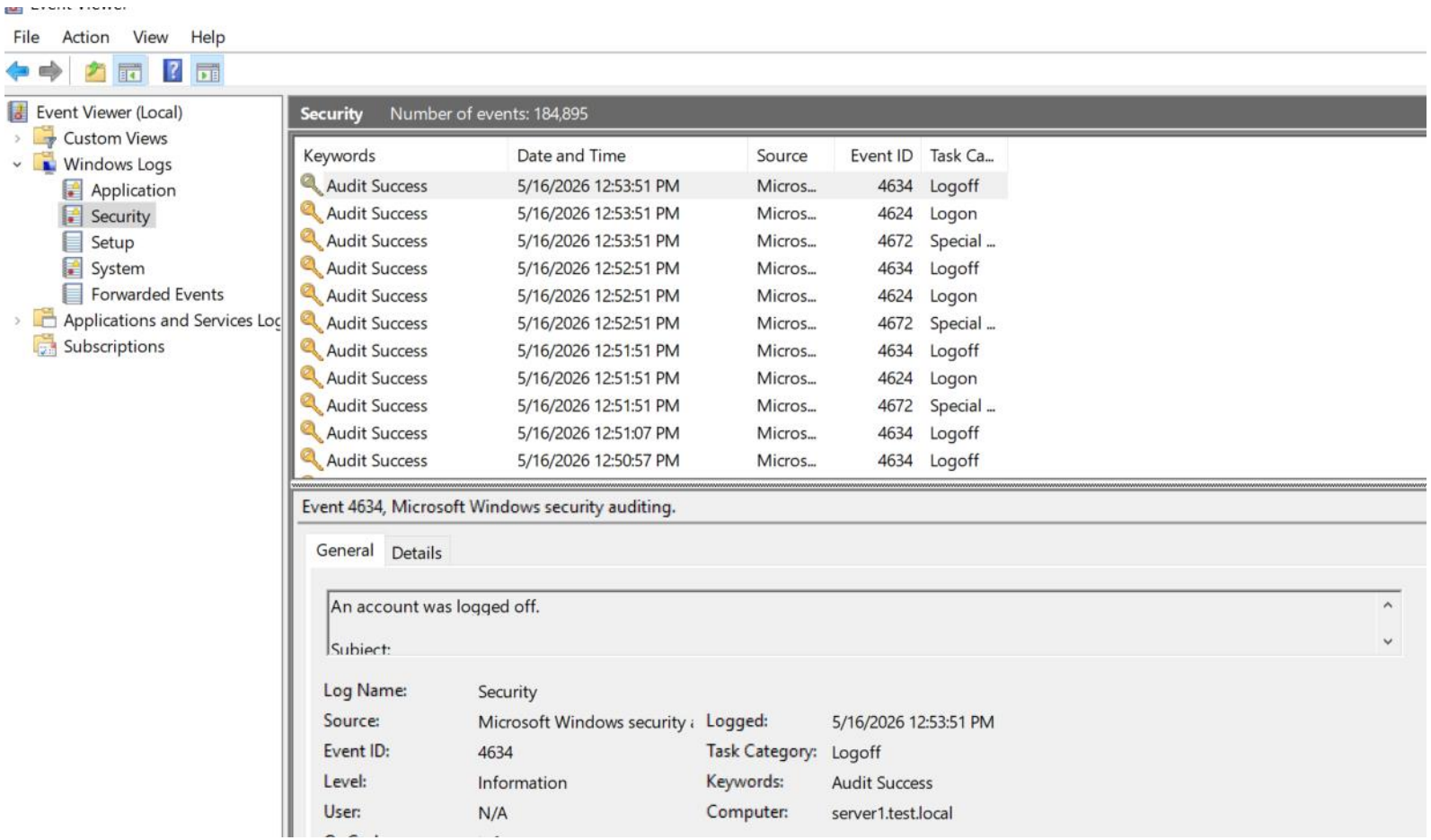
Reading 'Remote-Desktop-Management-Service/Admin' log ...

Recently Viewed Nodes

Name	Description	Modified	Created
Applications and Services ...	N/A	5/16/2026 12:51:06 PM	10/13/2025 4:52:06 PM
Windows Logs\Security	N/A	5/16/2026 12:51:11 PM	5/14/2025 7:17:19 AM

مهم‌ترین Event ID ها

- 4624 → Successful Logon
- 4625 → Failed Logon
- 4672 → Admin Logon
- 4720 → User Created
- 4728 → User added to Admin group
- 4740 → Account Lockout



فعال کردن LDAP Signing

- **LDAP Signing**برای تضمین **یکپارچگی (Integrity)** و جلوگیری از **دستکاری ترافیک LDAP**بین کلاینت و Domain Controllerاستفاده می‌شود.

- **مشکل وقتی LDAP Signing فعال نباشد**
- وقتی LDAP بدون signing کار کند، ترافیک می‌تواند در شبکه **Intercept یا Modify** شود. در این حالت مهاجم می‌تواند:
- حمله **Man-in-the-Middle (MITM)** انجام دهد
- درخواست‌های LDAP را **تغییر دهد**
- از حملات **NTLM Relay** استفاده کند
- احراز هویت را به سرور دیگر **Relay** کند و دسترسی بگیرد

- در بسیاری از حملات Active Directory، مهاجم ابتدا یک **NTLM Relay به LDAP** انجام می‌دهد و سپس:
- خود را به یک گروه Admin اضافه می‌کند
- ACL ها را تغییر می‌دهد
- دسترسی در AD ایجاد می‌کند
- **فعال کردن LDAP Signing جلوی این سناریو را می‌گیرد.**

تفاوت LDAP Signingو LDAPS

- این دو اغلب با هم اشتباه گرفته می‌شوند:

- **LDAP Signing**

- امضای دیجیتال روی پیام LDAP
- جلوگیری از تغییر داده

- **LDAPS**

- استفاده از **SSL/TLS (پورت 636)**
- رمزنگاری کامل ارتباط

- Group Policy Management

- Computer Configuration
- Policies
- Windows Settings
- Security Settings
- Local Policies
- Security Options

Group Policy Management Editor

File Action View Help

- Local Policies
  - Audit Policy
  - User Rights Assignment
  - Security Options
- Event Log
- Restricted Groups
- System Services
- Registry
- File System
- Wired Network (IEEE 802.3) Policies
- Windows Defender Firewall with Advanced Se
- Network List Manager Policies
- Wireless Network (IEEE 802.11) Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Active Directory (TEST.L
- Advanced Audit Policy Configuration
- Policy-based QoS
- Administrative Templates: Policy definitions (ADMX f
- Preferences

User Configuration
- Policies
- Preferences

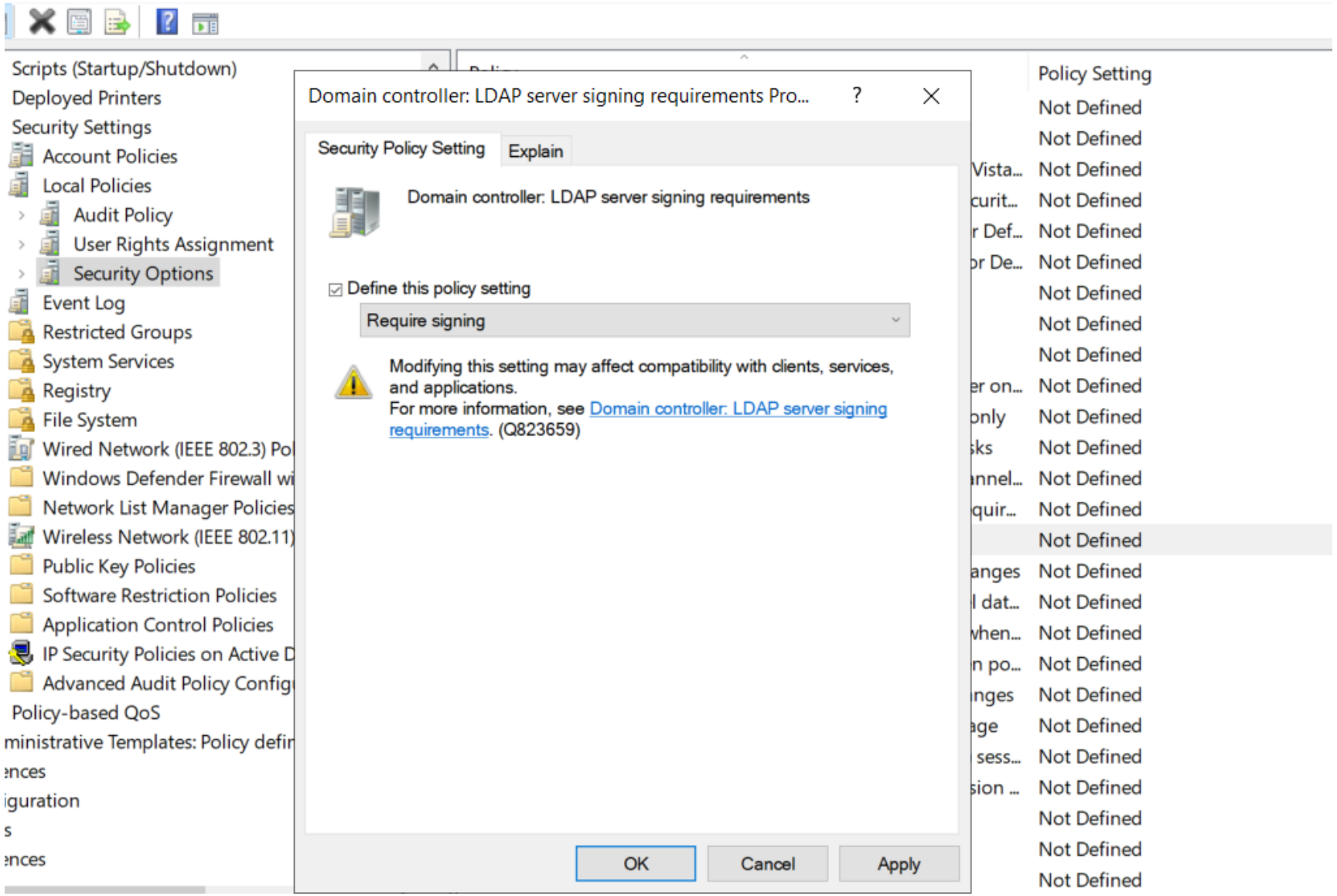
Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to cons...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vista...	Not Defined
Audit: Shut down system immediately if unable to log securit...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor Def...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor De...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user on...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure channel...	Not Defined
Domain controller: LDAP server channel binding token requir...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel dat...	Not Defined

• **Domain controller**: LDAP server signing requirements

e Action View Help

- Scripts (Startup/Shutdown)
- Deployed Printers
- Security Settings
  - Account Policies
  - Local Policies
    - Audit Policy
    - User Rights Assignment
    - Security Options
  - Event Log
  - Restricted Groups
  - System Services
  - Registry
  - File System
  - Wired Network (IEEE 802.3) Policies
  - Windows Defender Firewall with Advanced Se
  - Network List Manager Policies
  - Wireless Network (IEEE 802.11) Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Active Directory (TEST.L
  - Advanced Audit Policy Configuration
- Policy-based QoS
- Administrative Templates: Policy definitions (ADMX f
- Preferences
- User Configuration
- Policies
- Preferences

Policy	Policy Setting
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vista...	Not Defined
Audit: Shut down system immediately if unable to log securit...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor Def...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor De...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user on...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure channel...	Not Defined
Domain controller: LDAP server channel binding token requir...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel dat...	Not Defined
Domain member: Digitally encrypt secure channel data (when...	Not Defined
Domain member: Digitally sign secure channel data (when po...	Not Defined
Domain member: Disable machine account password changes	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) sess...	Not Defined
Interactive logon: Display user information when the session ...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Don't display last signed-in	Not Defined

• روی این حالت قرار می دیم :

- Require signing