TABLE I: Discovered fingerprints for various protocols.

Protocol	**No.**	**Condition**	**Field**	**Value**
TCP/IP	1	MF = 0, FSRA=0100	Frag, ...	(0, None, 0), ...
	2	MFSRA=00100, WS=e	WS	(6, 7, 8)
	3	MFSRA=00100, AO=e, ...	MSS	(1460, None, 1460)
	4	MFSRA=00100, TS=e	TS	(0, None, 0)
	5	FRA=001, TOS=0	Tos	(0, 0, None)
	6	FRA=001	Wnd	(0, 0, None)
	7	MFSRAEC=0010011, AO=e, ...	ECE	(1, None, 0)
	8	FRA=001, MD5=e	Frag, ...	(0, None, None)
	9	MFSRA=00100	TTL	(64, 64, 128)
	10	MFSRA=00100, WS=e	Wnd	(65535, 64240, 65535)
	11	MFSRAEC=0010011	ECE	(1, 1, 0)
	12	MFSRA=00100	Wnd	(65535, 64240, 65392)
	13	MR=00	Padding	(None, ”000000”, None)
	14	MFSRA=00100, SAckOK=e	TCPopt	(0, 1, 1)
	15	MRA=001	TCPopt	([], [], None)
	16	MFSRA=00100, SAckOK=e, ...	Frag	(None, None, 0)
	17	MFSRA=00100, AO=e, ...	Wnd	(65535, None, 65392)
	18	MrFSRAC=0101000, AO=e, ...	ECE	(0, None, 0)
	19	MFSRAECrr=001001100	ECE	(1, 0, 0)
	20	MFSRA=00100, MSS=e	Wnd	(65535, 64240, 64240)
	21	MRA=001	TOS	(0, 128, None)
	22	MRA=001	Frag	(0, 0, None)
	23	MFSRA=00100, WS=e	Wnd	(65535, None, 65535)
SNMP	1	M=0, comm=“public”, ...	PDU	(0, 1)
	2	version=0	PDU, v, ...	(None, e), ...
	3	M=0, v=2 or 3	PDU, v,...	(e, 0), ...
	4	v=0, ttl=3	ICMP	(e, None)
	5	v=1, comm=“public”	comm, len, ...	(None, “public”), ...
	6	M=0, v=2 or 3	MF, len, ...	(0, None), ...
ICMP	1	M=0	padding	(None, 00000, None)
	2	M=0	tos	(139, 139, None)
	3	M=0, unused=1	unused	(1, 0, None)
	4	M=0, unused=1	DF	(1, 0, None)
DNS	1	qr=0, opcode=1	qdcount	(0, 1, 1)
	2	qr=0, opcode=0, tc=0, rd=0, ad=1, cd=0	ad	(0, 1, 0)
	3	qr=0, aa=1	aa	(0, 0, 1)
	4	qr=0, opcode=1, rd=1	an	(None, RR*3, None)
	5	qr=0, tc=1	rcode	(4, 5, 1)
	6	qr=0, opcode=0, tc=1, ra=0	ra	(1, 1, 0)
	7	qr=0, opcode=0, tc=0, rd=0, ad=1, cd=0	ad	(0, 1, 1)
	8	qr=0, opcode=0, tc=1, rd=1	rcode	(0, 0, 1)
	9	qr=0, opcode=1, ra=0	ra	(0, 1, 0)
	10	qr=0, z=1	z	(0, 0, 1)
	11	qr=0, opcode=1, cd=1	cd	(0, 1, 1)
	12	qr=0, opcode=0, tc=0, rd=1	an	(0, 1, 2)
	13	qr=0, opcode=1, rd=1	ad	(0, 0, 1)
	14	qr=0, opcode=0, tc=0, rd=0	rcode	(0, 5, 5)
	15	qr=0, opcode=0, rd=0	an	(RR*3, None, None)
	16	qr=0, opcode=0, rd=0	arcount	(9, 0, 0)
	17	qr=0, opcode=1, tc=0	rcode	(4, 0, 4)
	18	qr=0, opcode=1, rd=1	ra	(0, 1, 1)

To be continued

The following abbreviations have been used for brevity: (1) M = MF, D = DF, F = FIN, S = SYN, R = RST, P = PSH, A = ACK, E = ECE, C = CWR, WS = WndScale, r = reserved, e = exist; (2) If the values are not static or too long to show in the table, we use 0, 1, 2 to mark different values.

TABLE II: Discovered fingerprints for various protocols (Continued).

Protocol	No.	Condition	Field	Value
UDP	1	dport=invalid	ICMP	(e, e, None)
NTP	1	complex	poll, ref, id, ...	(0, None), ...
	2	leap=0, version=3, ...	leap, ...	(None, 0), ...
	3	M=0	precision	(230, 232)
	4	version=3, mode=3, ...	poll	(0, 3)
TFTP	1	M=0, RR mode=‘octet’, tos=127	load, ttl,...	(None, e) ...
	2	M=0, opcode=1	DF	(1, 0) ...
	3	complex	padding	(0...00, 00)
	4	complex	padding, ...	(None, 00) ...
ARP	1	hwtype=1, ptype=2048, op=1	padding	(None, 00...0, None)
RIP	1	cmd=1, version=1	RIP header null	(0, 49240)
	2	complex	entrymatrix, ...	(None, 16)
ARP	1	RM=non ascii, RP=non ascii, ...	date, ...	(e, e, None)
	2	RM=’Get’, RP=valid	rawload	(0, 1, 2)
	3	RM=’Get’, RP=valid	contenttype	(0, 1, None)
	4	RM=non ascii	rawload	(0, 1, None)